

Sicherheit und mehr ...



**BusinessSolutions**



## Benutzerhandbuch

**MailGate UNIX**



---

# Inhaltsverzeichnis

<b>1</b>	<b>Über dieses Handbuch</b> .....	3
1.1	Einleitung .....	3
1.2	Aufbau des Handbuchs .....	4
1.3	Zeichen und Symbole .....	5
1.4	Abkürzungen .....	6
<b>2</b>	<b>Produktinformationen</b> .....	7
2.1	Leistungsumfang .....	8
2.2	Funktionsweise von AntiVir MailGate .....	9
2.3	Lizenzierungskonzept .....	11
2.4	Systemvoraussetzungen .....	12
<b>3</b>	<b>Installation</b> .....	13
3.1	Installationsdateien bereitstellen .....	14
3.2	Lizenzierung .....	15
3.3	Installation mit Installationsskript avinstall.pl .....	16
3.4	Manuelle Installation .....	22
3.5	Weitere Installationsschritte in Abhängigkeit vom MTA .....	25
3.6	AntiVir MailGate nach der Installation testen .....	32
3.7	AntiVir MailGate über grafische Installationsroutine installieren .....	33
<b>4</b>	<b>Bedienung</b> .....	42
4.1	AntiVir MailGate manuell starten und beenden .....	42
4.2	AntiVir MailGate manuell aktualisieren .....	44
4.3	Parameter für avgated und avgatefwd .....	44
4.4	Queue-Manager avq .....	46
4.5	Vorgehen bei Auffinden eines Virus oder unerwünschten Programms .....	47
<b>5</b>	<b>Konfiguration</b> .....	49
5.1	Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen .....	50
5.2	Konfigurieren der Datei avmailgate.conf .....	51
5.3	Konfigurieren der Datei avmailgate.acl .....	64
5.4	Virenspezifische Warnungen: Konfigurieren der Datei avmailgate.warn .....	65
5.5	Konfigurieren der Vorlagen für Nachrichten .....	66
5.6	Konfigurieren regelmäßiger Updates .....	68
5.7	Konfigurieren der Update-Nachrichten .....	71

---

<b>6</b>	<b>Grafische Benutzeroberfläche (GUI)</b> .....	73
6.1	Übersicht .....	73
6.2	AntiVir MailGate über GUI bedienen .....	74
6.3	AntiVir MailGate über GUI konfigurieren .....	79
6.3.1	Einstellungen für "normale" Benutzer .....	80
6.3.2	Einstellungen für Experten .....	87
<b>7</b>	<b>Service</b> .....	97
7.1	Support .....	97
7.2	Online-Shop .....	97
7.3	Kontakt .....	98
<b>8</b>	<b>Anhang</b> .....	99
8.1	Glossar .....	99
8.2	Weitere Infoquellen .....	100
8.3	Goldene Regeln zur Virenvorsorge .....	101

# 1 Über dieses Handbuch

In diesem Kapitel erhalten Sie einen Überblick über Aufbau und Inhalt des Handbuchs.

Nach einer kurzen Einleitung erhalten Sie Informationen zu folgenden Themen:

- [Aufbau des Handbuchs](#) – Seite 4
- [Zeichen und Symbole](#) – Seite 5
- [Abkürzungen](#) – Seite 6

## 1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen zu AntiVir MailGate zusammengestellt und führen Sie Schritt für Schritt durch Installation, Konfiguration und Bedienung der Software.

Im Anhang finden Sie ein Glossar, das Ihnen grundlegende Begriffe erläutert.

Weitere Informationen und Hilfestellung bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter (siehe [Service](#) – Seite 97).

Ihr Team von AntiVir


### 1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer AntiVir-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	Inhalt
<a href="#">1 Über dieses Handbuch</a>	Aufbau des Handbuchs, Zeichen, Symbole und Abkürzungen
<a href="#">2 Produktinformationen</a>	Allgemeine Hinweise zur Software AntiVir MailGate, zu Aufbau, Funktionsweise, Systemvoraussetzungen und Lizenzierung
<a href="#">3 Installation</a>	Anleitung zur Installation von AntiVir MailGate auf Ihrem System – sowohl Skript-basiert als auch über eine grafische Installationsroutine
<a href="#">4 Bedienung</a>	AntiVir manuell starten, beenden und aktualisieren, Vorgehen bei Auffinden eines Virus bzw. unerwünschten Programms
<a href="#">5 Konfiguration</a>	Anleitung zur optimalen Anpassung von AntiVir MailGate an Ihr System
<a href="#">6 Grafische Benutzeroberfläche (GUI)</a>	Allgemeine Hinweise zur GUI; Bedienung und Konfiguration von AntiVir MailGate über die GUI
<a href="#">7 Service</a>	Support und Service von H+BEDV Datentechnik GmbH
<a href="#">8 Anhang</a>	Glossar mit Erläuterungen zu Fachbegriffen und Abkürzungen, Goldene Regeln zur Vorsorge vor Viren und unerwünschten Programmen

## 1.3 Zeichen und Symbole

In diesem Handbuch werden folgende Zeichen und Symbole verwendet:

Symbol	Erläuterung
✓	... steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss
►	... steht vor einem Handlungsschritt, den Sie ausführen
↳	... steht vor einem Ergebnis, das direkt aus der vorangehenden Handlung folgt
	... steht vor einer Warnung bei Gefahr von kritischem Datenverlust oder Schäden an der Hardware
!	... steht vor einem Hinweis mit besonders wichtigen Informationen, z. B. zu den folgenden Handlungsschritten
i	... steht vor einem Tipp, der das Verständnis und die Nutzung von AntiVir MailGate erleichtert

Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

Hervorhebungen im Text	Erläuterung
<b>Strg</b> + <b>Alt</b>	Taste bzw. Tastenkombination
/usr/lib/AntiVir /usr/lib/AntiVir/antivir	Pfadangabe Dateiname
cd usr/lib/AntiVir	Eingabe des Anwenders
<b>Komponente auswählen</b> <b>Alles Markieren</b>	Elemente der Software-Oberfläche wie Menüpunkte, Fenstertitel, Schaltflächen in Dialogfenstern
<a href="http://www.antivir.de">http://www.antivir.de</a>	URL
Zeichen und Symbole – Seite ...	Querverweis innerhalb des Dokuments

### 1.4 Abkürzungen

In diesem Handbuch werden folgende Abkürzungen verwendet:

<b>Abkürzung</b>	<b>Erläuterung</b>
ACL	Access Control List
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
GPL	General Public License
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
PMS	Possible Malicious Software
RFC	Request For Comment
SMTP	Simple Mail Transfer Protocol
VDF	Virus Definition File



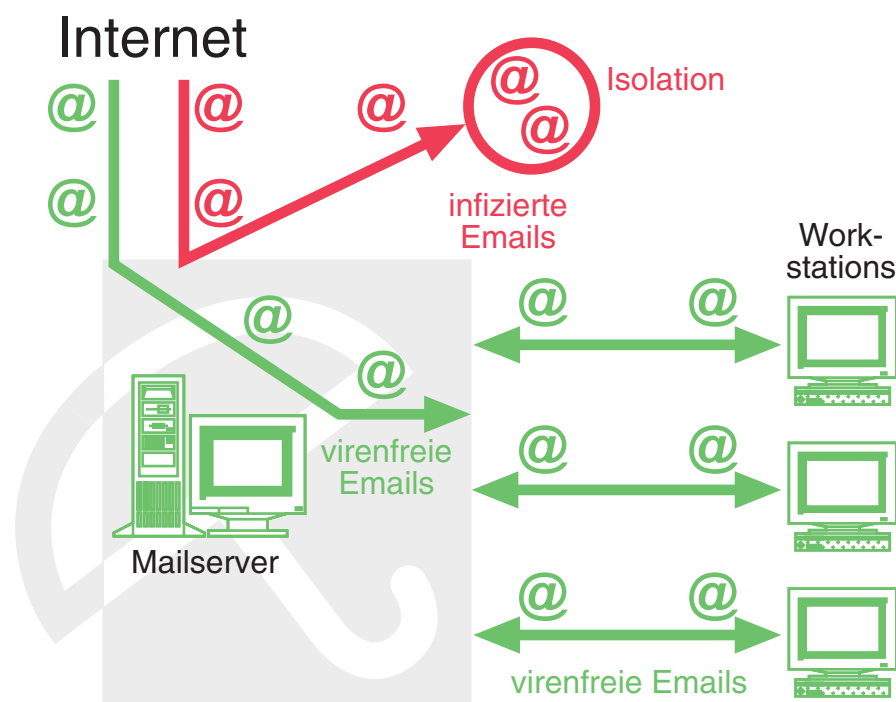
## 2 Produktinformationen

Der Datenverkehr per Email gehört zu den Selbstverständlichkeiten moderner Kommunikation und lässt sich aus dem Alltag nicht mehr wegdenken. Doch Emails transportieren auch immer öfter Viren bzw. unerwünschte Programme.

Viele dieser Viren bzw. unerwünschten Programme wurden zwar ausschließlich für den Angriff auf Windows-Betriebssysteme programmiert. Trotzdem stellen sie auch für Open-Source-Systeme eine Gefahr dar, denn Email-Server unter UNIX leiten die Malware ungehindert weiter. Dieses Schleusenprinzip bietet digitalen Angreifern eine willkommene Gelegenheit, sich ungehindert in Ihrem Netzwerk zu bewegen. Dabei können auch Windows-Clients mit Viren infiziert oder Rechner der Email-Partner geschädigt werden.

Immer öfter setzen kommerzielle Anwender auf UNIX. Doch mit dem Einzug der freien Software in Unternehmen und Behörden gerät das alternative Betriebssystem zunehmend ins Visier der Virenprogrammierer – der Schutz vor Computerviren wird sich in Zukunft auch unter UNIX als unverzichtbar erweisen. Deshalb haben wir AntiVir MailGate für UNIX entwickelt.

AntiVir MailGate prüft alle ein- und ausgehenden Emails (einschließlich Attachments) auf Ihrem UNIX-Mailserver auf Viren und unerwünschte Programme. Die Software läuft mit zahlreichen Mail Transport Agents (MTA), z. B. Sendmail, Postfix, Exim, Qmail und weiteren Programmen. Gängige Distributionen – Red Hat, SuSE, Debian u. a. – werden problemlos unterstützt.



Zwei ganz wichtige Hinweise gleich zu Beginn:



---

Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen.

- ▶ Fertigen Sie grundsätzlich regelmäßig Sicherungskopien (Backups) Ihrer Daten an.
- 



---

Ein Virenschutzprogramm ist nur dann zuverlässig und wirksam, wenn es aktuell ist.

- ▶ Stellen Sie die Aktualität von AntiVir MailGate über automatische Updates sicher. Sie erfahren in diesem Handbuch, was Sie hierfür tun müssen.
- 

## 2.1 Leistungsumfang

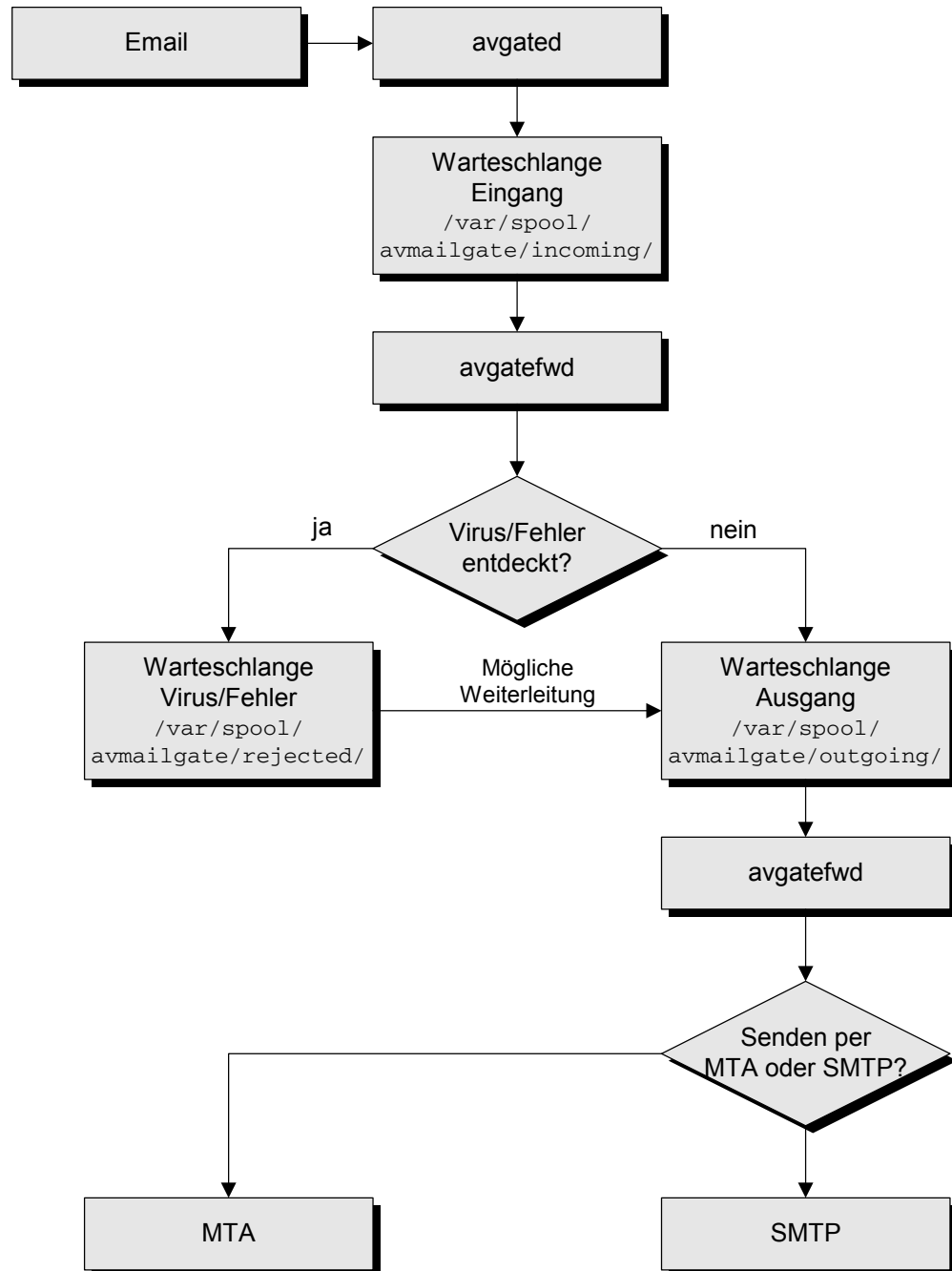
AntiVir MailGate bietet umfangreiche Konfigurationsmöglichkeiten, damit Sie die Kontrolle über den Email-Verkehr auf Ihrem System behalten.

Die wesentlichen Leistungsmerkmale von AntiVir MailGate im Überblick:

- Suche nach Viren und unerwünschten Programmen in Echtzeit
- Überprüfen ein- und ausgehender Emails
- Überprüfen von Postfächern
- Isolation von infizierten und verdächtigen Dateien
- Konfigurierbare Benachrichtigungsfunktionen für den Administrator sowie Absender und/oder Empfänger von Emails
- Logdatei als Protokoll über Email-Verkehr nutzbar
- Automatische Updates der Scan Engine und der VDF über das Internet
- Heuristische Makroviren-Erkennung
- Erkennt alle gebräuchlichen Archivtypen (mit einstellbarer Rekursionstiefe bei verschachtelten Archiven)
- Optional komfortable grafische Benutzeroberfläche (GUI) zur Bedienung und Konfiguration von AntiVir MailGate

## 2.2 Funktionsweise von AntiVir MailGate

AntiVir MailGate ist ein SMTP-Scanner, der alle ein- und ausgehenden Emails einschließlich deren Attachments auf Ihrem UNIX-Mailserver auf Viren und unerwünschte Programme prüft. Das Programm arbeitet mit hoher Geschwindigkeit und ist leicht zu konfigurieren.



Bei diesem so genannten Store-and-Forward-Agent teilen sich zwei Programme die Arbeit:

**avgated** Der SMTP-Dämon avgated nimmt die Emails entgegen, filtert diese und legt sie im Spool-Verzeichnis ab. Dieses Programm kann als eigenständiger Server laufen, der den Port 25 (SMTP) belegt, oder durch die Internetsuperdämonen inetd oder xinetd gestartet werden.

**avgatefwd** Der Forwarder-Dämon avgatefwd liest die im Spool-Verzeichnis zwischengespeicherten Emails, dekodiert vorhandene Attachments und startet anschließend die Suche nach Viren und unerwünschten Programmen.

Sind die Emails ohne Virenbefund, werden sie sofort weitergeleitet. Eine als infiziert erkannte Email wird nicht weitergeleitet, sondern im Spool-Verzeichnis (rejected) abgelegt.

Entsprechend der Konfiguration in der Datei avmailgate.conf werden dort auch verdächtige Emails abgelegt, z. B. Emails mit Passwort-geschützten Archiven und fragmentierte Emails.

Über das Queue Manager Skript avq (zum Durchsuchen des Spool-Verzeichnisses, siehe Kapitel [Queue-Manager avq](#) – Seite 46) können die Warteschlangen bei Bedarf geprüft werden.

**Warnungen** Beim Fund von Viren bzw. unerwünschten Programmen sowie verdächtigen Dateien erhält der Postmaster eine Email mit detaillierter Warnung. Zusätzlich können auch Absender und/oder Empfänger der Email benachrichtigt werden. Das Programm enthält Templates für die Warnungen, die Sie Ihren Bedürfnissen anpassen können. Außerdem werden Statusmeldungen via syslog ausgegeben.

**Grafische Benutzeroberfläche (GUI)** Die grafische Benutzeroberfläche (GUI) unterstützt Sie bei der Konfiguration von AntiVir MailGate und stellt den laufenden Überwachungsprozess grafisch dar. AntiVir MailGate ist aber auch ohne GUI voll funktionsfähig und vollständig konfigurierbar.

Für die GUI benötigen Sie Java 1.4.0 oder höher.

## 2.3 Lizenzierungskonzept

Um AntiVir MailGate zu nutzen, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an  
(siehe [http://www.antivir.de/dateien/antivir/handbuch/pdf/eula\\_antivir.pdf](http://www.antivir.de/dateien/antivir/handbuch/pdf/eula_antivir.pdf)).

Sie können die vielfältigen Funktionen von AntiVir MailGate mit folgenden Lizenz-Modellen nutzen:

- Demoversion
- Vollversion
- Komfortpaket

Die Lizenzierung ist abhängig von der Anzahl der Benutzer im Netzwerk, die durch AntiVir MailGate geschützt werden sollen.

Die Lizenz wird über die Lizenzdatei avmgate.key vergeben. Diese erhalten Sie von H+BEDV per Email. Sie enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Sie kann also auch die Lizenz für mehrere Produkte von H+BEDV enthalten.

Demoversion	Ohne Lizenzdatei läuft AntiVir MailGate als Demoversion. Dabei wird in jede Email ein Werbebanner von H+BEDV eingefügt. Ein automatisches Update ist nicht möglich, d. h. neue Virendefinitionsdateien und eine neue AntiVir Search Engine müssen immer manuell von der Webseite heruntergeladen werden.
Evaluation Version	Nähere Informationen zur Evaluation Version erhalten Sie auf unserer Webseite <a href="http://www.antivir.de">http://www.antivir.de</a> .
Vollversion	<p>Zum Leistungsumfang einer Vollversion gehören:</p> <ul style="list-style-type: none"> <li>• Bereitstellung der AntiVir-Version zum Download aus dem Internet</li> <li>• Lizenzdatei per Email zur Freischaltung von der Demoversion auf die Vollversion</li> <li>• Ausführliche Installationsanleitung (digital)</li> <li>• Bereitstellung von PDF-Handbüchern zum Download aus dem Internet</li> <li>• Vierwöchiger Installationssupport ab Kaufdatum</li> <li>• Newsletter-Service (per Email)</li> <li>• Update-Service auf die Programmdateien und die VDF per Internet</li> </ul>

- Komfortpaket    Das Komfortpaket enthält zusätzlich zur lizenzierten Vollversion:
- Alle drei Monate: Kostenlose Lieferung einer bootfähigen CD-ROM mit dem AntiVir Rescue-System und allen aktuellen AntiVir-Programmen
  - Umfangreiches Installationshandbuch (gedruckt) bei der Erstauslieferung
  - Lizenzdatei auf Diskette bei der Erstauslieferung
  - Newsletter-Service (gedruckt, Versand per Post)

## 2.4 Systemvoraussetzungen

AntiVir MailGate stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an den Server (abhängig vom Email-Verkehr, von der Anzahl und Größe der Attachments etc. kann temporär auch mehr Speicherplatz nötig sein):



Die Versionen für UNIX Server, UNIX Workstation, FreeBSD, OpenBSD und Sun Sparc Solaris unterscheiden sich weder bei der Installation noch in der Handhabung (bis auf einige Dateinamen).

---

- Rechner ab i486
- 8 MB freier Speicherplatz auf der Festplatte
- 20 MB temporärer Speicherplatz auf der Festplatte
- 32 MB freier Hauptspeicher (empfohlen: 64 MB)
- Linux mit GLIBC oder LIBC5 bzw. FreeBSD (Intel), OpenBSD (Intel) oder Sun Sparc Solaris

Wenn Sie die GUI verwenden wollen:

- Zusätzlich Java 1.4.0 oder höher

## 3 Installation

Die aktuelle Version von AntiVir MailGate ist im Internet verfügbar. Wenn Sie im Rahmen des Komfortpakets eine AntiVir-CD-ROM besitzen, können Sie die Dateien auch von dieser installieren.

AntiVir MailGate wird als gepacktes Archiv zur Verfügung gestellt.

Sie können das Programm entweder **manuell oder mit dem Installationsskript** avinstall.pl auf Ihrem System installieren.

Vorausset-  
zungen

Für die Installation von AntiVir MailGate müssen Sie als **root** angemeldet sein. Voraussetzung ist außerdem ein lauffähiger MTA (Sendmail, Postfix, Exim, Qmail etc.) auf Ihrem System. Für Probleme mit der Konfiguration, die nicht direkt AntiVir MailGate betreffen, übernehmen wir keinen Support.

Beispielhaft wird in diesem Kapitel eine Installation mit einer "Standard"-Sendmail-Konfiguration auf einer SuSE-Distribution beschrieben. Wenn Sie das Programm in Kombination mit einem anderen MTA installieren oder zum Beispiel in Kombination mit Lotus Domino verwenden, finden Sie weitere Informationen in den zugehörigen Dateien (INSTALL.sendmail, INSTALL.exim, INSTALL.qmail, INSTALL.postfix etc.).

Dieses Kapitel ist in folgende Abschnitte untergliedert:

- [Installationsdateien bereitstellen](#) – Seite 14
- [Lizenzierung](#) – Seite 15
- [Installation mit Installationsskript avinstall.pl](#) – Seite 16
- [Manuelle Installation](#) – Seite 22
- [Weitere Installationsschritte in Abhängigkeit vom MTA](#) – Seite 25
- [AntiVir MailGate nach der Installation testen](#) – Seite 32
- [AntiVir MailGate über grafische Installationsroutine installieren](#) – Seite 33

### 3.1 Installationsdateien bereitstellen

#### Programmdatei aus dem Internet laden

- ▶ Laden Sie die aktuelle Datei von unserer Webseite <http://www.antivir.de> auf Ihren lokalen Rechner. Zurzeit heißt diese Datei `antivir-mailgate-prof-<version>.tar.gz` (ohne grafische Installationsroutine) bzw. `antivir-mailgate-linux-gui_installer.tar.gz` (mit grafischer Installationsroutine).
- ▶ Kopieren Sie die Datei in ein Verzeichnis Ihrer Wahl auf dem Computer ab, auf dem MailGate laufen soll, z. B. nach `/tmp`.

#### Programmdatei von CD-ROM laden

- ▶ Wählen Sie auf Ihrer CD-ROM den Ordner `/DE/PRODUCTS/UNIX/MAILGATE/` bzw. `/DE/PRODUCTS/UNIX/GUI_INSTALLERS/`.
- ▶ Kopieren Sie die Datei `antivir-mailgate-prof-<version>.tar.gz` bzw. `antivir-mailgate-linux-gui_installer.tar.gz` in ein Verzeichnis Ihrer Wahl auf dem Computer, auf dem MailGate laufen soll, z. B. nach `/tmp`.

#### Programmdatei entpacken

Beispielhaft wird das Entpacken der Datei ohne grafische Installationsroutine beschrieben.

- ▶ Wechseln Sie in das temporäre Verzeichnis:  

```
cd /tmp
```
- ▶ Entpacken Sie die Archivdatei für das AntiVir-Paket:  

```
tar xzvf antivir-mailgate-prof-<version>.tar.gz
```

  - ↳ Ein Verzeichnis `antivir-mailgate-prof-<version>` wird im temporären Verzeichnis angelegt.



## 3.2 Lizenzierung

Sie müssen AntiVir MailGate lizenzieren, um es in vollem Umfang nutzen zu können (siehe [Lizenzierungskonzept](#) – Seite 11). Hierfür benötigen Sie die Lizenzdatei avmgate.key, die auf einer Diskette oder per Email geliefert wird. Sie enthält Informationen zu Umfang und Dauer der Lizenz. Ohne Lizenzdatei läuft AntiVir MailGate ausschließlich als Demoversion mit reduziertem Leistungsumfang.

### Lizenz erwerben

- ▶ Kontaktieren Sie uns telefonisch oder per Email ([info@antivir.de](mailto:info@antivir.de)), um eine gültige Lizenzdatei zu erhalten.
  - ↳ Sie erhalten die Lizenzdatei per Email zugesandt.
- ▶ Sie können AntiVir auch einfach und schnell über unseren Online-Shop erwerben (weitere Informationen siehe <http://www.antivir.de>).

### Lizenzdatei kopieren

- ▶ Kopieren Sie die Lizenzdatei avmgate.key in Ihr Installationsverzeichnis /tmp/antivir-mailgate-prof-<version>.



Sie können die Installation zunächst auch ohne Lizenzdatei durchführen. AntiVir MailGate läuft dann als Demoversion.

Die Lizenzdatei kann jederzeit nachträglich in das Programmverzeichnis /usr/lib/AntiVir/ kopiert werden.

---

### 3.3 Installation mit Installationsskript avinstall.pl

Mit dem Installationsskript avinstall.pl läuft die Installation von AntiVir MailGate weitgehend automatisch ab.

Das Skript führt folgende Aufgaben durch:

- Prüfen der Installationsdateien auf Vollständigkeit
- Prüfen, ob Sie ausreichende Rechte zur Installation besitzen
- Prüfen, inwieweit schon eine Version von AntiVir MailGate auf dem Rechner vorhanden ist
- Kopieren der Programmdateien (bereits vorhandene veraltete Dateien werden überschrieben)
- Kopieren der Konfigurationsdateien (bereits vorhandene Dateien werden beibehalten)
- Optional: Installieren des Internet Updater
- Optional: Installieren der grafischen Benutzeroberfläche (GUI)

Wenn Sie AntiVir MailGate manuell installieren wollen, können Sie dieses Kapitel überspringen. Lesen Sie dann weiter im Kapitel [Manuelle Installation](#) – Seite 22.

#### Installation vorbereiten

- ✓ Programmdatei wurde aus dem Internet oder von CD-ROM geladen und entpackt.
- Loggen Sie sich als **root** ein. Andernfalls haben Sie keine ausreichende Berechtigung für die Installation und das Skript bricht mit folgender Fehlermeldung ab:

```
You must be root, to execute this script.
```

- Wechseln Sie in das Verzeichnis, in das Sie AntiVir MailGate entpackt haben, also z. B.:

```
cd /tmp/antivir-mailgate-prof-<version>
```

## AntiVir MailGate installieren

Sind Verzeichnisse oder Dateien bereits vorhanden, erscheinen während der Installation Meldungen wie die folgende:

```
...  
Found existing /etc/avmailgate.conf. Skipping.  
...
```

- ▶ Geben Sie ein:  
`perl avinstall.pl`  
↳ Das Installationsskript wird gestartet.
- ▶ Um AntiVir MailGate installieren zu können, müssen Sie zunächst die Lizenzbestimmungen lesen.
- ▶ Verlassen Sie die Datei mit den Lizenzbestimmungen mit `q`.  
↳ Folgende Abfrage erscheint:

```
Do you agree the LICENSE [n]:
```

- ▶ Geben Sie `y` ein und bestätigen Sie mit `[Enter]`.  
↳ Anschließend werden Sie nach dem Pfad für die manual pages gefragt:

```
Enter the path where the manual pages will be located  
[/usr/share/man]:
```

- ▶ Bestätigen Sie die Standardeinstellung mit `[Enter]` oder geben Sie einen neuen Pfad ein.  
↳ Wenn keine Lizenzdatei gefunden wurde, werden Sie anschließend nach dem Pfad für die Lizenzdatei gefragt:

```
Enter the path to your license file []:
```

- ▶ Geben Sie den Pfad zu Ihrer Lizenzdatei an und bestätigen Sie mit `[Enter]`.  
– ODER –

Wenn Sie MailGate zunächst als Demoversion ohne Lizenzdatei installieren wollen:

- ▶ Bestätigen Sie mit `[Enter]`.

- ↳ Anschließend werden Sie gefragt, ob Sie den automatischen Internet Updater installieren wollen:

```
An automatic internet updater of AntiVir for UNIX is
available. This is a daemon that will run in the back-
ground and automatically check for updates (internet
access is required).
```

```
You may also manually check for updates using:
```

```
antivir --update
```

```
You do not need to install the automatic internet
updater in order to manually check for updates. Please
read the README file for more information on updates
and how they can best suit you.
```

```
Install the automatic internet updater? [n]:
```



Der Internet Updater ist nicht notwendig, um Updates zu erhalten. Sie können jederzeit mit AntiVir ein manuelles Update über das Internet starten. Hinweise hierzu unter [AntiVir MailGate manuell aktualisieren](#) – Seite 44.

Für die Erstinstallation wird aber eine Installation des Internet Updater empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren.

---

Wenn Sie den Internet Updater installieren wollen (empfohlen):

- Geben Sie `y` ein und bestätigen Sie mit `[Enter]`.

- ↳ Der Internet Updater wird in `/usr/lib/AntiVir` installiert. Anschließend werden Sie gefragt, ob der Internet Updater beim Systemstart automatisch gestartet werden soll:

```
Would you like the automatic updater to start auto-
matically? [y]
```

- Bestätigen Sie mit `[Enter]`. Sie können diese Einstellung später wieder rückgängig machen.

- ↳ Das Programm nimmt die Einstellungen in der Datei /etc/crontab vor (siehe [Konfigurieren regelmäßiger Updates](#) – Seite 68), wobei die Update-Zeit automatisch vom Programm gewählt wird.

```
Installing new queuemanager script to:
/usr/lib/AntiVir/avq
Creating link from /usr/lib/AntiVir/avq to
/usr/sbin/avq

Installing new /usr/lib/AntiVir/antivir with version:
6.29.0.130
Installing new /usr/lib/AntiVir/antivir.vdf with ver-
sion 6.29.0.130

Installing new /usr/lib/AntiVir/avgated with version:
2.0.2-14+gui
Creating link from /usr/lib/AntiVir/avgated to
/usr/sbin/avgated

Installing new /usr/lib/AntiVir/avgatefwd with ver-
sion: 2.0.2-14+gui
Creating link from /usr/lib/AntiVir//avgatefwd to
/usr/sbin/avgatefwd

Installing config file /etc/avmailgate.conf

Installing config file /etc/antivir.conf

Installing ignore file for addressfilter
/etc/avmailgate.ignore

Installing scan file for addressfilter
/etc/avmailgate.scan

Installing warn file /etc/avmailgate.warn

Enter the hosts and/or domains that are local:
[domain.de my.domain.de]:
```

- Ändern Sie ggf. die Einstellungen und bestätigen Sie mit **[Enter]**.  
↳ Die folgende Abfrage erscheint:

```
Enter the hosts and networks that are allowed to
relay:
[127.0.0.1/8 192.168.0.0/16]:
```

- Ändern Sie ggf. die Einstellungen und bestätigen Sie mit **[Enter]**.

- ↳ Anschließend werden Sie gefragt, ob AntiVir MailGate beim Systemstart automatisch gestartet werden soll:

```
Installing config file /etc/avmailgate.acl  
  
Installing start/stop script for a SuSE System  
  
Would you like AvMailGate to start automatically? [n]
```

- Geben Sie `y` ein und bestätigen Sie mit `[Enter]`. Sie können diese Einstellung später rückgängig machen.

– ODER –

Bestätigen Sie die Standardeinstellung `n` mit `[Enter]`.

- ↳ Anschließend werden Sie gefragt, ob MailGate mit der grafischen Benutzeroberfläche (GUI) installiert werden soll (nur auf Linux-Systemen):

```
Installing /usr/local/man/man5/avmailgate.conf.5  
Installing /usr/local/man/man8/avmailgate.8  
  
Would you like to enable GUI support?  
The GUI allows you to monitor real time activity, view  
logs, and configure MailGate. [y]
```



AntiVir MailGate wird mit einer GUI bereit gestellt, die es ermöglicht, die Echtzeit-Aktivitäten zu überwachen, Logeinträge anzuzeigen und das Produkt zu konfigurieren. MailGate ist aber auch ohne GUI voll funktionsfähig.

---

Wenn Sie die GUI installieren wollen:

- ✓ Java 1.4.0 oder höher muss auf dem Rechner installiert sein.
- Bestätigen Sie die Frage nach der GUI-Installation mit `[Enter]`.
  - ↳ Die Programmdateien für die GUI werden kopiert.
  - ↳ AntiVir MailGate ist damit installiert. Sie erhalten folgende Meldung:

```
AntiVir MailGate is now installed. Please read the  
installation description in the directory avmailgate  
and follow the instructions in INSTALL.sendmail,  
INSTALL.qmail, INSTALL.postfix or INSTALL.exim.  
Then start AntiVir MailGate "/usr/lib/AntiVir/avmail-  
gate start".
```

- ▶ Je nachdem, welchen MTA Sie nutzen, setzen Sie die Installation fort wie im Kapitel [Weitere Installationsschritte in Abhängigkeit vom MTA](#) – Seite 25 beschrieben.
- ▶ Anschließend können Sie AntiVir MailGate starten:  

```
/usr/lib/AntiVir/avmailgate start
```

### AntiVir MailGate erneut installieren

Sie können das Installationsskript `avinstall.pl` jederzeit neu aufrufen. Hiermit sind folgende Vorgänge möglich:

- Installation einer neuen Version (Upgrade). Das Installationsskript prüft die bestehende Version und installiert notwendige neue Komponenten. Einstellungen, die Sie in den Konfigurationsdateien vorgenommen haben (siehe [Konfiguration](#) – Seite 49), werden dabei nicht überschrieben, sondern übernommen.
- Aktivierung oder Deaktivierung des automatischen Starts des Internet Updater.

Das Vorgehen ist für alle Fälle gleich:

- ▶ Wechseln Sie in das Verzeichnis, in das Sie AntiVir MailGate entpackt haben, also z. B.:  

```
cd /tmp/antivir-mailgate-prof-<version>/
```
- ▶ Geben Sie ein:  

```
perl avinstall.pl
```

  - ↳ Das Installationsskript läuft weitgehend ab wie oben beschrieben.
- ▶ Ändern Sie die entsprechenden Einstellungen während der Installation.

AntiVir MailGate ist mit den neuen Einstellungen installiert.

### 3.4 Manuelle Installation

#### Installation vorbereiten

- ✓ Ein lauffähiger MTA (Sendmail, Postfix, Exim, Qmail etc.) muss auf Ihrem System installiert sein.
- ✓ Programmdatei wurde aus dem Internet oder von CD-ROM geladen und entpackt.
- ▶ Loggen Sie sich als **root** ein. Andernfalls haben Sie keine ausreichende Berechtigung für die Installation.
- ▶ Wechseln Sie in das Verzeichnis antivir-mailgate-prof-<version>/avmailgate:  

```
cd antivir-mailgate-prof-<version>/avmailgate/
```

#### Verzeichnisse anlegen und Dateien kopieren



---

Achten Sie auf die Groß- und Kleinschreibung des Wortes "AntiVir".

---

- ▶ Erstellen Sie das Verzeichnis /usr/lib/AntiVir:  

```
mkdir /usr/lib/AntiVir
```
- ▶ Kopieren Sie die Virensignaturdatei vdf/antivir.vdf in das Verzeichnis /usr/lib/AntiVir/:  

```
cp vdf/antivir.vdf /usr/lib/AntiVir/
```
- ▶ Setzen Sie die Rechte aller User und Groups auf uucp:  

```
chown uucp:antivir /usr/lib/AntiVir
```

```
chown uucp:antivir /usr/lib/AntiVir/antivir.vdf
```
- ▶ Kopieren Sie die Scan-Engine antivir in das Verzeichnis /usr/lib/AntiVir. Setzen Sie User und Group auf uucp:  

```
cp bin/<Betriebssystem>/antivir /usr/lib/AntiVir/
```

```
chown uucp:antivir /usr/lib/AntiVir/antivir
```
- ▶ Kopieren Sie die Programmdateien avgated und avgatefwd in das Verzeichnis /usr/lib/AntiVir:  

```
cp bin/<Betriebssystem>/avgated /usr/lib/AntiVir/
```

```
cp bin/<Betriebssystem>/avgatefwd /usr/lib/AntiVir/
```
- ▶ Erstellen Sie Links von /usr/lib/AntiVir/avgated und /usr/lib/AntiVir/avgatefwd nach /usr/sbin/:  

```
ln -s /usr/lib/AntiVir/avgated /usr/sbin/avgated
```

```
ln -s /usr/lib/AntiVir/avgatefwd /usr/sbin/avgatefwd
```



- Kopieren Sie die Konfigurationsdateien `avmailgate.conf`, `avmailgate.acl` und `antivir.conf` in das Verzeichnis `/etc`:

```
cp etc/avmailgate.conf /etc/  
cp etc/avmailgate.acl /etc/  
cp etc/antivir.conf /etc/
```

- Editieren Sie die Konfigurationsdateien, nachdem Sie die manpages gelesen haben (per Standardeinstellung müssen Sie nur die Datei `avmailgate.acl` editieren).
- Erstellen Sie das Spool-Verzeichnis `/var/spool/avmailgate/`. Das Spool-Verzeichnis darf nur für den in `/etc/avmailgate.conf` spezifizierten User und die eingestellte Gruppe zugänglich sein (Standardeinstellung: `uucp:antivir`). Die Rechte müssen dabei auf 700 gesetzt werden.

```
mkdir /var/spool/avmailgate  
chown uucp:antivir /var/spool/avmailgate  
chmod 700 /var/spool/avmailgate  
cd /var/spool/avmailgate/
```

- Erstellen Sie im Spool-Verzeichnis die Queue-Verzeichnisse `incoming`, `outgoing` und `rejected`. Die Verzeichnisse dürfen nur für den in `/etc/avmailgate.conf` spezifizierten User und die eingestellte Gruppe zugänglich sein (Standardeinstellung: `uucp:antivir`). Die Rechte müssen dabei auf 700 gesetzt werden.

```
mkdir incoming  
mkdir outgoing  
mkdir rejected  
chown uucp:antivir *  
chmod -R 700 *
```

## Lizenzdatei kopieren

Wenn Sie eine Lizenz für den privaten oder kommerziellen Gebrauch besitzen:

- Kopieren Sie die Lizenzdatei `avmgate.key` in das Verzeichnis `/usr/lib/AntiVir`:

```
cp avmgate.key /usr/lib/AntiVir/  
chown uucp:antivir /usr/lib/AntiVir/avmgate.key
```



Ohne Lizenzdatei läuft AntiVir MailGate als Demoversion. Dabei wird in jede Email ein Werbebanner von H+BEDV Datentechnik GmbH eingefügt. Ein automatisches Update ist nicht möglich, d. h. neue Virendefinitionsdateien und eine neue Scan Engine müssen immer manuell von der Webseite heruntergeladen werden.

---

### AntiVir MailGate starten

- ▶ Beenden Sie Sendmail, falls es als Dämon läuft:

```
killall sendmail
```

- ▶ Starten Sie AntiVir MailGate:

```
/usr/lib/AntiVir/avgated
```

```
/usr/lib/AntiVir/avgatefwd
```

### Zugriffsrechte kontrollieren

Wenn Sie die User- und Group-Parameter in der Konfigurationsdatei `avmailgate.conf` ändern:

- ▶ Stellen Sie sicher, dass die folgenden Dateien die gleichen Zugriffsrechte besitzen:

```
/usr/lib/AntiVir/antivir
```

```
/usr/lib/AntiVir/antivir.vdf
```

```
/usr/lib/AntiVir/avmgate.key
```

- ▶ Stellen Sie sicher, dass die folgenden Verzeichnisse die gleichen Zugriffsrechte besitzen:

```
/usr/lib/AntiVir/
```

```
/var/spool/avmailgate/
```

```
/var/spool/avmailgate/incoming/
```

```
/var/spool/avmailgate/outgoing/
```

```
/var/spool/avmailgate/rejected/
```

### AntiVir MailGate automatisch starten und stoppen

- ▶ Kopieren Sie das zu Ihrer Distribution passende Skript (für SuSE 8.x `rc.avgate.SuSE8x`) in das `init`-Verzeichnis Ihres Systems.
- ▶ Erzeugen Sie die entsprechenden symbolischen Links für die Run-level.

Beispiel:  
SuSE8.1

- ▶ Führen Sie die folgenden Befehle aus:

```
cp rc.avgate.SuSE8x /etc/init.d/avgate
```

```
cd /etc/init.d
```

```
ln -sf ../avgate rc2.d/S20avgate
```

```
ln -sf ../avgate rc2.d/K20avgate
```

```
ln -sf ../avgate rc3.d/S20avgate
```

```
ln -sf ../avgate rc3.d/K20avgate
```

```
ln -sf ../avgate rc5.d/S20avgate
```

```
ln -sf ../avgate rc5.d/K20avgate
```

## Update automatisieren

Wie Sie Ihre Scan Engine und vdf-Datei stets auf dem aktuellen Stand halten, erfahren Sie im Kapitel [Konfigurieren regelmäßiger Updates](#) – Seite 68.

## 3.5 Weitere Installationsschritte in Abhängigkeit vom MTA

Sie haben AntiVir MailGate bereits wie oben beschrieben installiert – mit dem Installationsskript `avinstall.pl` oder manuell. Je nachdem, mit welchem MTA Sie arbeiten, sind noch einige manuelle Anpassungen nötig.

Nachfolgend werden die MTAs Sendmail, Exim, Qmail und Postfix beschrieben.

### Sendmail konfigurieren



Wenn Sie mit Sendmail arbeiten, empfehlen wir Ihnen, AntiVir Milter statt AntiVir MailGate einzusetzen. Damit ist gewährleistet, dass die SMTP-Funktionalität von Sendmail vollständig erhalten bleibt (z. B. SMTP-Authentifizierung).

Eine vorhandene Lizenzdatei für MailGate können Sie auch problemlos für Milter einsetzen.

Es gibt zwei Möglichkeiten für die Arbeit von AntiVir MailGate mit Sendmail:

- Backdoor-Mechanismus
- Weiterleitung per Sendmail

Backdoor-  
Mechanismus

✓ Sendmail läuft als Dämon

Wenn Sendmail installiert ist und an Port 25 lauscht, müssen Sie dies ändern, da bereits AntiVir MailGate den Port 25 nutzt. Sie können Sendmail z. B. so konfigurieren, dass es an Port 825 lauscht. AntiVir MailGate kann über den `ForwardTo`-Eintrag in der Datei `avmailgate.conf` so eingestellt werden, dass Emails direkt an einen Port weitergeleitet werden. Per Standardeinstellung wird die Weiterleitung von Emails über den Aufruf von `/usr/lib/sendmail` vorgenommen.

Sie müssen folgende Einstellungen vornehmen:

- Fügen Sie in der Datei `/etc/services` folgende Zeile ein:

```
smtp-backdoor 825/tcp
```

- ▶ Ändern Sie in der Datei `/etc/sendmail.cf` die Zeile `#O DaemonPortOptions=Name=MTA` wie folgt:
    - `DaemonPortOptions=Name=MTA, Port=smtp-backdoor`
  - ODER –
  - Ändern Sie bei älteren Versionen in der Datei `/etc/sendmail.cf` die Zeile `#O DaemonPortOptions=Port=smtp` wie folgt:
    - `DaemonPortOptions=Port=smtp-backdoor`
  - ▶ Starten Sie Sendmail neu:
    - `killall -HUP sendmail`
  - ▶ Legen Sie fest, wie Emails weitergeleitet werden sollen. Suchen Sie in der Datei `/etc/avmailgate.conf` die Einträge unter `# Select how mail should be forwarded.`
  - ▶ Ändern Sie diese Einträge wie folgt:
    - `# ForwardTo /usr/sbin/sendmail -oem -oi`
    - `# Or if you want the mail to be sent by SMTP`
    - `ForwardTo SMTP: localhost port smtp-backdoor`
- Weiterleitung per Sendmail
- ✓ Sendmail darf nicht als Dämon gestartet werden.
  - ▶ Editieren Sie die Datei `/etc/avmailgate.conf` wie folgt:
    - `ForwardTo /usr/sbin/sendmail -oem -oi`

## Exim konfigurieren

AntiVir MailGate arbeitet mit Exim ab Version 3.0 zusammen.

Um Ihre Exim-Version festzustellen:

- ▶ Geben Sie ein:
  - `exim -bV`

Es gibt zwei Möglichkeiten für die Arbeit von AntiVir MailGate mit Exim:

- AntiVir MailGate wird als Content-Filter in Exim eingebunden (empfohlen)
- Proxy-Modus

Content-Filter

### **AntiVir MailGate konfigurieren:**

- ▶ Ändern Sie in der Datei `avmailgate.conf` folgende Einträge (bzw. fügen Sie diese Einträge hinzu):
  - `ListenAddress 127.0.0.1 port 10024`
  - `ForwardTo SMTP: 127.0.0.1 port 10025`
- ▶ Starten Sie AntiVir MailGate neu.

## Exim konfigurieren:

- Ändern Sie in der Datei `exim.conf` folgenden Eintrag (bzw. fügen Sie diesen Eintrag hinzu):

```
# Listen on all interfaces on port 25
# and on 127.0.0.1 port 10025
local_interfaces = 0.0.0.0.25 : 127.0.0.1.10025
```

## Router-Eintrag hinzufügen:

- Suchen Sie in der Datei `exim.conf` nach dem Eintrag `begin router` und fügen Sie folgende Einträge hinzu:

```
# Router for AntiVir MailGate
antivir_mailgate:
    debug_print = "R: AntiVir MailGate for
    $local_part@$domain"
    driver = manualroute
    transport = antivir_mailgate_transport
    route_list = "* localhost byname"
    self = send
    # do not call this router in the second instance
    of Exim
    condition = ${if !eq
    {$interface_port}{10025}{1}{0}}
```

## Transport-Eintrag hinzufügen:

- Suchen Sie in der Datei `exim.conf` nach dem Eintrag `begin transports` und fügen Sie folgende Einträge hinzu:

```
# Transport for AntiVir MailGate
antivir_mailgate_transport:
    driver = smtp
    # connect to port 10024
    port = 10024
    allow_localhost
```

- Starten Sie Exim neu.

## Proxy-Modus AntiVir MailGate konfigurieren:

- Ändern Sie in der Datei `avmailgate.conf` folgende Einträge (bzw. fügen Sie diese Einträge hinzu):

```
ListenAddress      0.0.0.0 port 25
ForwardTo SMTP:    127.0.0.1 port 825
```

- Starten Sie AntiVir MailGate neu.

### Exim konfigurieren:

- ▶ Ändern Sie in der Datei `exim.conf` folgenden Eintrag (bzw. fügen Sie diesen Eintrag hinzu):  
`daemon_smtp_port = 825`
- ▶ Starten Sie Exim neu.

### Qmail konfigurieren

Es gibt zwei Möglichkeiten für die Arbeit von AntiVir MailGate mit Qmail:

- Sendmail-wrapper
- Backdoor-Mechanismus



Ändern Sie SMTP zu SMTP-Backdoor nur in der `run`-Datei. Alle anderen Parameter sind nur Beispiele.

---

#### Sendmail-wrapper

Emails können über den `sendmail-wrapper`, der mit Qmail mitgeliefert wird, ausgeliefert werden (Standardeinstellung). Gehen Sie dafür nach der Qmail-Installationsanleitung vor und machen Sie diesen wrapper verfügbar.

- ▶ Machen Sie den `sendmail-wrapper` von Qmail verfügbar:  

```
ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```
- ▶ Legen Sie fest, wie Emails weitergeleitet werden sollen. Suchen Sie dafür in der Datei `/etc/avmailgate.conf` die Einträge unter `# Select how mail should be forwarded.`
- ▶ Ändern Sie diese Einträge wie folgt:  

```
# Send mail by piping it thru sendmail (this is the default)

ForwardTo /usr/sbin/sendmail -oem -oi

# Or if you want the mail to be sent by SMTP

# ForwardTo SMTP: localhost port smtp-backdoor
```

#### Backdoor-Mechanismus

Die zweite Möglichkeit besteht darin, Emails über den Port 825 zu verschicken, an dem Qmail lauschen muss. Dies lässt sich z. B. über `inetd.conf` einstellen (siehe Qmail-Installationsanleitung).

- ▶ Fügen Sie in der Datei `/etc/services` folgende Zeile ein:  
`smtp-backdoor 825/tcp`

- Legen Sie fest, wie Emails weitergeleitet werden sollen. Suchen Sie dafür in der Datei `/etc/avmailgate.conf` die Einträge unter `# Select how mail should be forwarded.`

- Ändern Sie diese Einträge wie folgt:

```
# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
ForwardTo SMTP: localhost port smtp-backdoor
```

Wenn Sie `inetd` zusammen mit Qmail nutzen:

- Fügen Sie in der Datei `inetd.conf` folgende Zeilen ein (eine Zeile!):

```
smtp-backdoor stream tcp nowait qmaild /var/qmail/bin/
tcp-env tcp-env /var/qmail/bin/qmail-smtpd
```

Wenn Sie `tcpwrapper` zusammen mit Qmail nutzen:

- Ändern Sie in der Datei `/var/qmail/supervise/qmail-smtpd/run` den Port für Qmail. Suchen Sie beispielsweise folgende Zeile:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/
qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/
qmail-smtpd 2>&1
```

- Ändern Sie die Zeile wie folgt:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/
qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp-backdoor /var/
qmail/bin/qmail-smtpd 2>&1
```

### Postfix konfigurieren

Unter Postfix gibt es zwei Möglichkeiten, AntiVir MailGate einzubinden:

- AntiVir MailGate wird als Content-Filter in Postfix eingebunden (empfohlen)
- AntiVir MailGate lauscht am Port 25 und gibt die Emails an Postfix weiter

Content-Filter Seit Snapshot 20000520 von Postfix ist es möglich, AntiVir MailGate als Content-Filter einzubinden. Ein Release mit den Möglichkeiten des Content-Filtering gibt es seit Version 20010228. Gehen Sie wie folgt vor:

- Fügen Sie in der Datei `etc/services` folgende Einträge hinzu:

```
# Content Filter for postfix
antivir 10024/tcp #Port for avgated
smtp-backdoor 10025/tcp #Port for postfix backdoor
```

- Suchen Sie in der Datei `/etc/avmailgate.conf` die Einträge unter `# Select interface and port, the smtp daemon will listen on.`

- Ändern Sie diese Einträge wie folgt:

```
# Select interface and port, the smtp daemon will listen on.

# Port may be given as a number or a service name.
ListenAddress localhost port antivir

# Select how mail should be forwarded.

# Send mail by piping it thru sendmail (this is the default)

# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
ForwardTo SMTP: localhost port smtp-backdoor
```

Wenn Sie den SuSE-Mail-Server II nutzen:

- Ändern Sie die Zeile `#AllowSourceRouting NO` wie folgt:

```
AllowSourceRouting YES
```

- Beenden Sie AntiVir MailGate und starten Sie es neu:

```
/sbin/init.d/avgate restart
oder
/etc/init.d/avgate restart
```



- Fügen Sie in der Datei `/etc/postfix/master.cf` folgenden Eintrag hinzu:

```
# service type private unpriv chroot wakeup maxproc com-  
mand + args  
  
# (yes) (yes) (yes) (never) (50)  
  
smtp inet n - n - - smtpd  
  
Für AntiVir Maildämon  
  
localhost:smtp-backdoor inet n - n - - smtpd -o  
content_filter= (eine Zeile!)
```

- Stellen Sie sicher, dass das erste Zeichen in der Tabelle kein Leerzeichen und kein Tab ist.

Der Eintrag `smtpd -o content_filter` deaktiviert die entsprechende Zeile in einer zweiten Instanz von Postfix (andernfalls kommt es zu einem mail loop).

- Fügen Sie in der Datei `/etc/postfix/main.cf` folgenden Eintrag hinzu:

```
# AntiVir Einbindung  
  
content_filter = smtp:127.0.0.1:10024
```
- Starten Sie Postfix neu:

```
/etc/init.d/postfix restart  
  
oder  
  
/etc/init.d/postfix reload
```



Wenn Emails nach der Installation von AntiVir MailGate von Postfix in den Status **deferred** gesetzt werden:

- Suchen Sie in der Datei `main.cf` nach der Zeile

```
defer_transports = local
```
  - Kommentieren Sie die Zeile aus:

```
# defer_transports = local
```
-

- Lauschen am Port 25
- ▶ Suchen Sie in der Datei `master.cf` nach der Zeile  
`smtp inet n - n - - smtpd`
  - ▶ Kommentieren Sie diese Zeile aus:  
`# smtp inet n - n - - smtpd`
    - ↳ Dies verhindert, dass Postfix am SMTP-Port lauscht. Statt dessen kann `avgated` an diesem Port lauschen. Emails, die von `avgated` weitergeleitet werden, werden vom `sendmail-wrapper /usr/lib/sendmail` (bei Postfix mitgeliefert) abgearbeitet.
  - ▶ Starten Sie Postfix neu:  
`/etc/init.d/postfix restart`  
oder  
`/etc/init.d/postfix reload`

### 3.6 AntiVir MailGate nach der Installation testen

Es wird empfohlen, nach der Installation die Funktionsfähigkeit von AntiVir MailGate zu testen. Sie können dies mit einem Testvirus namens Eicar tun, der von allen Virenscannern erkannt wird. Der Testvirus richtet keinerlei Schaden an, löst aber bei korrekter Installation (und Konfiguration) auf Ihrem Rechner eine Reaktion des Email-Scanners aus.

- ▶ Kopieren Sie die folgende Zeichenkette in eine Datei:  
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`  
– ODER –  
Laden Sie die Eicar-Datei von der Webseite <http://www.eicar.com> herunter.
- ▶ Schicken Sie diese Datei als Attachment einer Test-Email an AntiVir MailGate.
- ▶ Prüfen Sie die Reaktionen im Verzeichnis  
`/var/spool/avmailgate/rejected`.
- ▶ Prüfen Sie die Meldungen, die AntiVir MailGate an Ihre Logdatei oder an syslog ausgibt.

### 3.7 AntiVir MailGate über grafische Installationsroutine installieren

Sie können AntiVir MailGate auch komfortabel über eine grafische Installationsroutine installieren. Dafür müssen Sie die entsprechende Datei heruntergeladen haben, wie im Kapitel [Installationsdateien bereitstellen](#) – Seite 14 beschrieben.



Die grafische Installationsroutine dient nur der Installation. Sie steht in keinem Zusammenhang mit der GUI, über die AntiVir MailGate bedient und konfiguriert werden kann.



AntiVir MailGate mit grafischer Installationsroutine ist nur für Linux verfügbar. Es wird Java 1.4.0 oder höher benötigt.

✓ Die Programmdatei wurde entpackt und liegt im Verzeichnis `/tmp/antivir-mailgate-linux-gui_installer`

► Geben Sie ein:

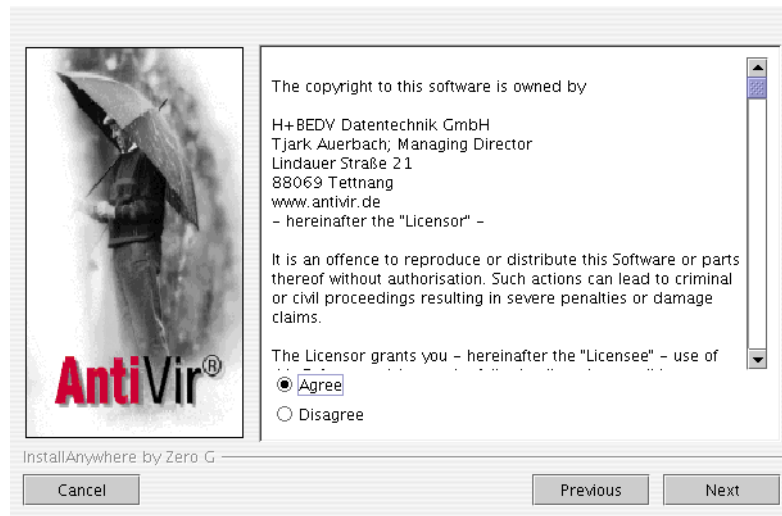
`./install`

↳ Es erscheint ein Begrüßungstext und eine kurze Beschreibung des Programms.



► Klicken Sie auf **Next**.

↳ Das folgende Dialogfenster mit den Lizenzbedingungen erscheint:

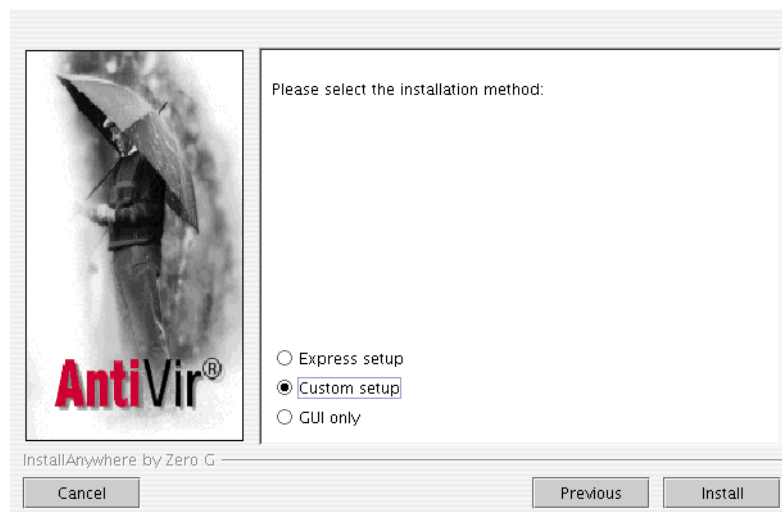


**i**

Um die Installation fortzusetzen, müssen Sie die Lizenzbedingungen akzeptieren. Wenn **Disagree** aktiviert ist, kann die Installation nicht fortgesetzt werden.

► Aktivieren Sie die Option **Agree** und bestätigen Sie mit **Next**.

↳ Das folgende Dialogfenster erscheint:



Sie haben drei Möglichkeiten, MailGate zu installieren:

- **Express setup:** Das Programm wird mit einer vorgegebenen Grundeinstellung installiert.
- **Custom setup:** Das Programm wird benutzerdefiniert installiert.
- **GUI only:** Es wird nur die GUI im Verzeichnis `usr/lib/AntiVir` installiert.

### Express setup

Das Programm wird mit folgender Grundeinstellung installiert:

- "MailGate-Hauptprogramm" und "AntiVir Engine" werden in folgendes Verzeichnis installiert:

```
usr/lib/AntiVir
```

- Die VDF wird in folgendes Verzeichnis installiert:

```
/usr/lib/AntiVir/antivir.vdf
```

- avgated und avgatefwd Binarys werden in folgendes Verzeichnis installiert:

```
/usr/lib/AntiVir/avgated
```

```
/usr/lib/AntiVir/avgatefwd
```

- Es wird kein automatischer Internet Updater installiert.
- Die GUI-Unterstützung ist aktiviert.
- MailGate wird beim Booten des Rechners nicht automatisch gestartet.
- Es wird keine Lizenzdatei kopiert, d. h. MailGate arbeitet zunächst als Demoversion.

- ▶ Aktivieren Sie **Express setup** und klicken Sie auf **Install**.

↳ Ein Dialogfenster erscheint, in dem alle Einstellungen und weitere Anweisungen angezeigt werden.

- ▶ Klicken Sie auf **Next**.

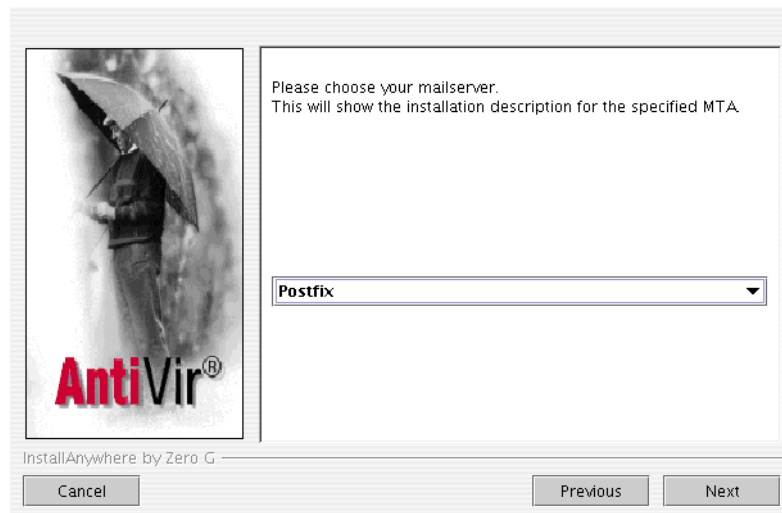
↳ Das Programm wird installiert.

- ▶ Klicken Sie im abschließenden Dialogfenster auf **Done**, um die Installation abzuschließen.

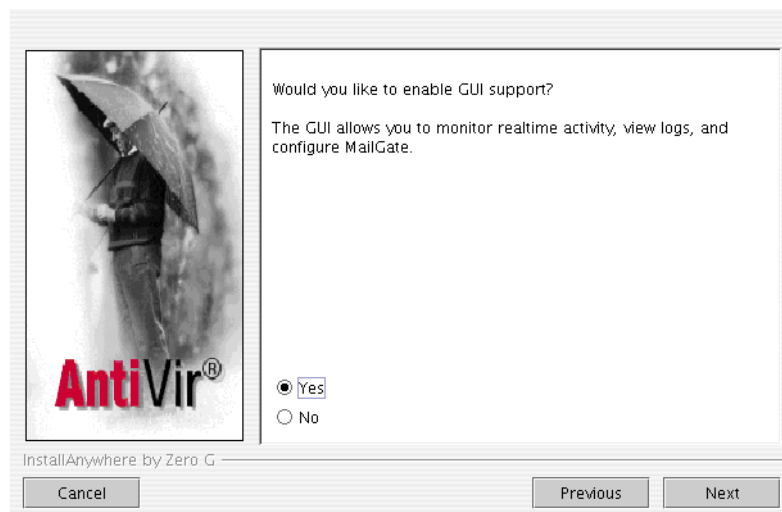
### Custom setup

Sie können das Programm auch mit benutzerdefinierten Einstellungen installieren.

- ▶ Aktivieren Sie **Custom setup** und klicken Sie auf **Next**.
  - ↳ Im folgenden Dialogfenster wird abgefragt, welcher Mailserver benutzt wird (Postfix, Sendmail, Exim, Qmail etc.):

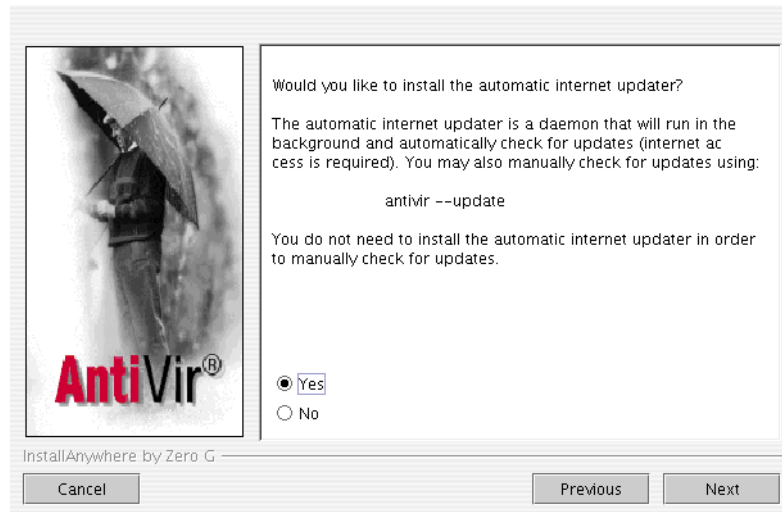


- ▶ Wählen Sie Ihren Mailserver und klicken Sie auf **Next**.
  - ↳ Im folgenden Dialogfenster wird abgefragt, ob die GUI-Unterstützung aktiviert werden soll (Eintrag in der Datei avmailgate.conf):



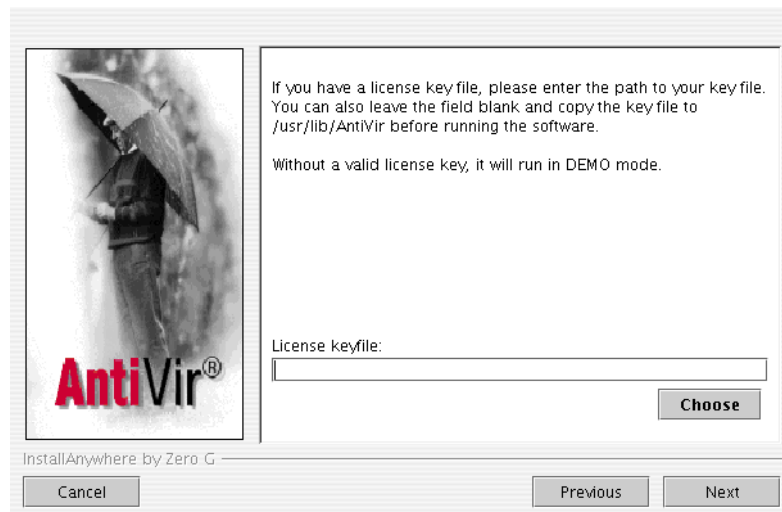
- ▶ Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.

- ↳ Im folgenden Dialogfenster wird abgefragt, ob der automatische Internet Updater installiert werden soll:



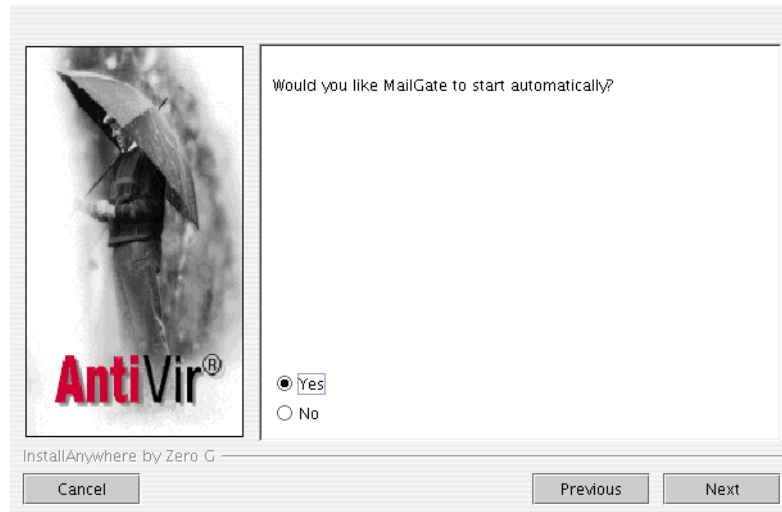
Wenn der Internet Updater installiert werden soll:

- ▶ Aktivieren Sie **Yes** und klicken Sie auf **Next** (in diesem Fall erscheint am Ende der Installation die Abfrage, ob der Internet Updater beim Booten des Rechners automatisch gestartet werden soll).
- ↳ Im folgenden Dialogfenster wird abgefragt, ob eine Lizenzdatei kopiert werden soll:

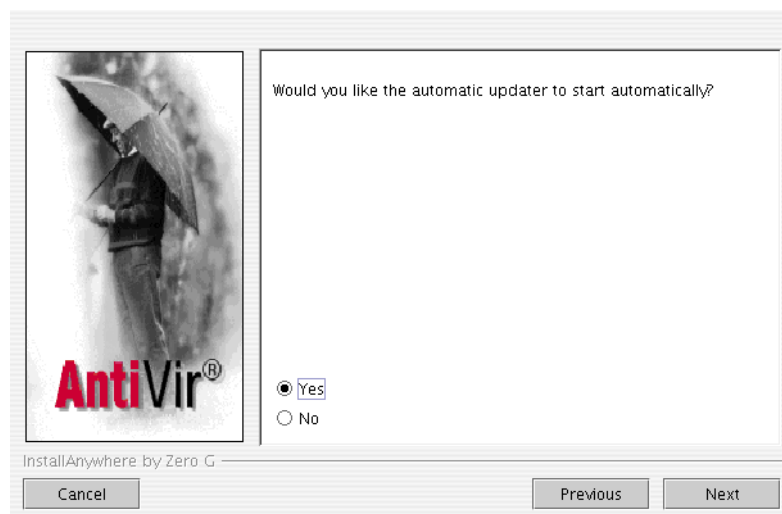


- ▶ Folgen Sie den Anweisungen und klicken Sie auf **Next**.

- ↳ Im folgenden Dialogfenster wird abgefragt, ob MailGate beim Booten des Rechners automatisch gestartet werden soll:



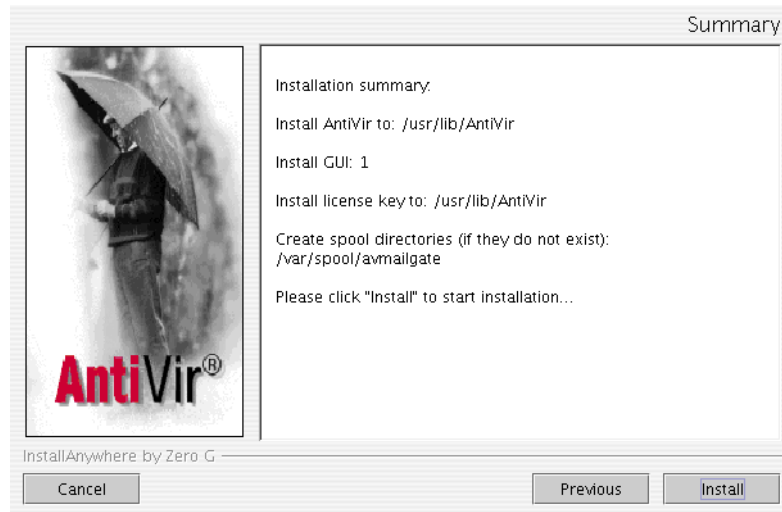
- ▶ Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.
  - ↳ Optional wird im folgenden Dialogfenster abgefragt, ob der Internet Updater beim Booten des Rechners automatisch gestartet werden soll:



- ▶ Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.



- ↳ Ein Dialogfenster erscheint, in dem alle Einstellungen und weitere Anweisungen angezeigt werden:



- ▶ Klicken Sie auf **Install**.
  - ↳ Das Programm wird installiert.

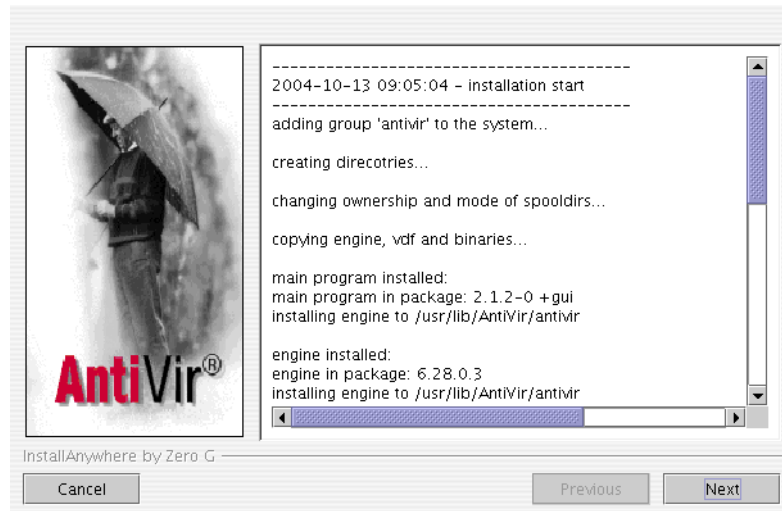
### GUI only

Wählen Sie diese Installationsart, wenn Sie nur die GUI installieren wollen.

- ▶ Aktivieren Sie **GUI only** und klicken Sie auf **Next**.
  - ↳ Die GUI wird im folgenden Verzeichnis installiert:  
`/usr/lib/AntiVir`
    - ↳ Ein Dialogfenster erscheint, in dem alle Einstellungen und weitere Anweisungen angezeigt werden.
- ▶ Klicken Sie auf **Install**.
  - ↳ Die GUI wird installiert.

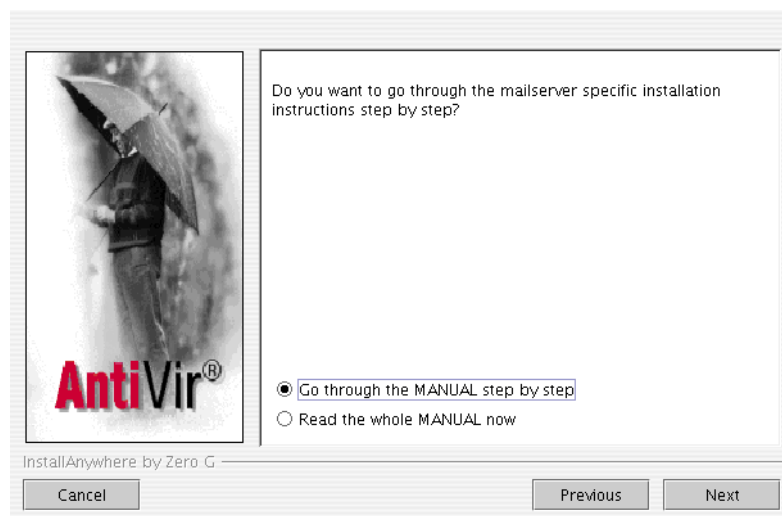
### Installation abschließen

Unabhängig davon, welche Installationsart Sie gewählt haben, erscheint ein Dialogfenster, in dem die einzelnen Installationsschritte aufgelistet sind:



► Klicken Sie auf **Next**.

↳ Das folgende Dialogfenster erscheint nur, wenn Sie zu Beginn der Installation einen Mailserver gewählt haben:

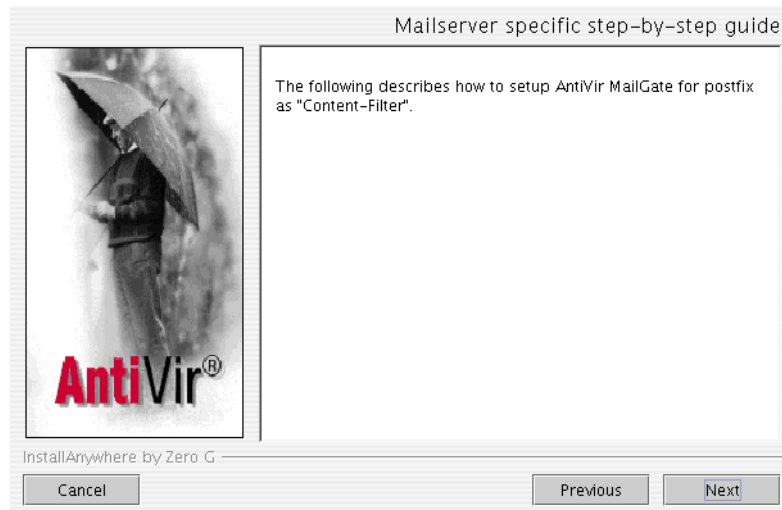


Sie haben die Möglichkeit, entweder den Anweisungen des gewählten Mailservers "Schritt für Schritt" zu folgen oder alles auf einmal zu lesen. Je nach Mailserver unterscheiden sich die Installationsanweisungen.

Nachfolgend ein Beispiel für Postfix:

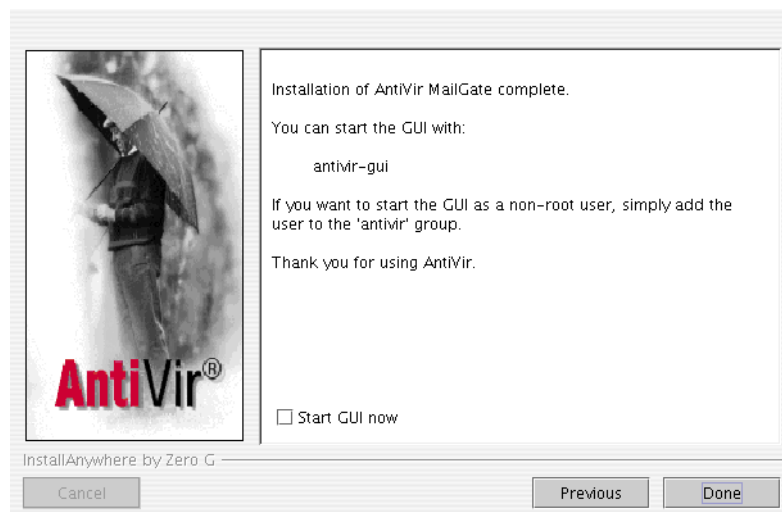
- Wählen Sie **Go through the MANUAL step by step** und klicken Sie auf **Next**.

↳ Beispiel Postfix: Das folgende Dialogfenster erscheint:



- Klicken Sie auf **Next**.

↳ Das folgende Dialogfenster erscheint:



Wenn Sie die GUI direkt starten wollen:

- Aktivieren Sie das Kontrollkästchen **Start GUI now**.
- Klicken Sie auf **Done**.

Die Installation ist abgeschlossen.

# 4 Bedienung

Nach Abschluss der Installation und Konfiguration ist die laufende Überwachung Ihres Systems durch AntiVir MailGate gewährleistet. Im laufenden Betrieb werden unter Umständen gelegentliche Änderungen der Konfiguration sinnvoll sein, die Sie gemäß [Konfiguration](#) – Seite 49 vornehmen.

In bestimmten Fällen können manuelle Aufrufe von AntiVir MailGate oder eine manuelle Behandlung der von AntiVir MailGate gefilterten Emails notwendig sein. In diesem Kapitel wird Folgendes beschrieben:

- [AntiVir MailGate manuell starten und beenden](#) – Seite 42
- [AntiVir MailGate manuell aktualisieren](#) – Seite 44
- [Parameter für avgated und avgatefwd](#) – Seite 44
- [Queue-Manager avq](#) – Seite 46

Zusätzlich erhalten Sie Informationen über:

- [Vorgehen bei Auffinden eines Virus oder unerwünschten Programms](#) – Seite 47

## 4.1 AntiVir MailGate manuell starten und beenden

Wenn Sie AntiVir MailGate so installiert haben wie in [Installation](#) – Seite 13 beschrieben, startet das Programm beim Systemstart und wird beim Herunterfahren gestoppt.

Dennoch kann es notwendig sein, AntiVir MailGate manuell zu starten oder zu stoppen. Insbesondere eine Änderung in den Konfigurationsdateien macht einen Neustart erforderlich, damit die Änderungen wirksam werden.

Das Skript `/usr/lib/AntiVir/avmailgate` vereinfacht Starten und Beenden der MailGate-Dämonen.



Sie müssen als **root** oder mit entsprechenden Zugriffsrechten eingeloggt sein, um AntiVir MailGate manuell starten und beenden zu können.

---

## AntiVir Mailgate starten

- Geben Sie ein:

```
/usr/lib/AntiVir/avmailgate start
```

- ↳ Das Programm startet mit folgender Meldung:

```
Initializing SMTP port. (AvMailGate)..done
```

## AntiVir Mailgate beenden

- Geben Sie ein:

```
/usr/lib/AntiVir/avmailgate stop
```

- ↳ Das Programm wird mit folgender Meldung beendet:

```
Shutting down SMTP port (AvMailGate):..done
```

## AntiVir MailGate neu starten

Dieser Befehl ist z. B. nach einer Modifikation der Konfigurationsdateien sinnvoll.

- Geben Sie ein:

```
/usr/lib/AntiVir/avmailgate restart
```

- ↳ Das Programm wird mit folgender Meldung beendet und neu gestartet:

```
Shutting down SMTP port (AvMailGate):..done  
Initializing SMTP port (AvMailGate):..done
```

## Status von AntiVir MailGate abfragen

- Geben Sie ein:

```
/usr/lib/AntiVir/avmailgate status
```

- ↳ Eine Information zum Status der MailGate-Dämonen wird ausgegeben, z. B.:

```
Checking for service AvMailGate: running
```

### 4.2 AntiVir MailGate manuell aktualisieren

AntiVir kann jederzeit manuell aktualisiert werden.

Es wird empfohlen, AntiVir zum Aktualisieren als **root** laufen zu lassen.

Vorteil: Eventuell laufende Prozesse der AntiVir-Dämonen (z. B. den AntiVir Guard, SAVAPI, MailGate) werden automatisch mit den aktualisierten Virenschutzdateien geladen, ohne laufende Scanprozesse zu unterbrechen. Es ist also sichergestellt, dass alle Dateien gescannt werden.

Wenn AntiVir zum Aktualisieren nicht als **root** gestartet wird, besitzt es nicht die notwendigen Rechte, um die AntiVir-Dämonen neu zu starten. Der Neustart muss dann von **root** manuell vorgenommen werden.

Wenn Sie AntiVir aktualisieren wollen:

- Geben Sie ein:

```
/usr/lib/AntiVir/antivir --update
```

Wenn Sie lediglich prüfen wollen, ob eine neue Version von AntiVir vorliegt, ohne AntiVir zu aktualisieren:

- Geben Sie ein:

```
/usr/lib/AntiVir/antivir --update --check
```

### 4.3 Parameter für avgated und avgatefwd

avgated und avgatefwd können auch direkt aufgerufen werden. Dies sollte im Normalbetrieb allerdings nicht notwendig sein.

Im Folgenden eine Kurzreferenz der möglichen Parameter, die die Einstellungen in avmailgate.conf außer Kraft setzen.

## Parameter für avgated

Parameter	Erklärung
-V oder --version	Gibt die Versionsnummer aus
-C config-file	Definiert eine alternative Konfigurationsdatei statt der Standardeinstellung /etc/avmailgate.conf
-A acl-file	Definiert eine alternative acl-Datei statt der Standardeinstellung /etc/avmailgate.acl
-i	avgated läuft im inetd-Modus mit SMTP-Konversation über stdin und stdout. Nähere Informationen über die Arbeitsweise siehe inetd(8).
-p port	Definiert den Port, an dem avgated statt des normalen SMTP Port (25) lauscht.

Die folgenden Optionen werden während des Debugging verwendet:

Parameter	Erklärung
-D debug-level	Setzt den Debug-Level
-R remote.host	Definiert den Remote-Host-Domänen-Namen (Voraussetzung: -i)
-r remote-ip-addr	Definiert die Remote-Host-IP-Adresse (aaa.bbb.ccc.ddd) (Voraussetzung: -i)
-q port	Definiert den Remote-Host-TCP-Port

## Parameter für avgatefwd

Parameter	Erklärung
-V oder --version	Druckt die Versionsnummer
-C config-file	Definiert eine alternative Konfigurationsdatei statt der Standardeinstellung /etc/avmailgate.conf
-A acl-file	Definiert eine alternative acl-Datei statt der Standardeinstellung /etc/avmailgate.acl
-D debug-level	Setzt den Debug-Level

### 4.4 Queue-Manager avq

Über den Queue-Manager avq kann gezielt auf das Spool-Verzeichnis von AntiVir MailGate /var/spool/avmailgate/ und seine Unterverzeichnisse zugegriffen werden. Der Status der hier abgelegten Emails (siehe [Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen](#) – Seite 50) kann abgefragt und manuell verändert werden.

#### Status der Emails in der Queue abfragen

- ▶ Geben Sie ein  
`/usr/lib/AntiVir/avq`  
↳ Der Status aller Emails in der Queue wird ausgegeben.

#### Emails aus der Queue löschen



---

Das Löschen von Emails aus der Queue ist im Wesentlichen für infizierte Emails sinnvoll. Weitergeleitete Emails werden automatisch aus der Queue gelöscht.

---

- ▶ Ermitteln Sie die ID der Email. Im Falle von infizierten Emails gibt AntiVir MailGate diese ID in seinen Meldungen und in seinen Email-Benachrichtigungen an den Postmaster an.
- ▶ Geben Sie ein (ID steht dabei für die ID der betreffenden Email):  
`/usr/lib/AntiVir/avq --remove=ID`  
↳ Die Email wird aus der Queue gelöscht.

#### Weiterleitung von Emails erzwingen



---

Bei diesem Vorgehen werden unter Umständen gefährliche Viren weitergeleitet.

- ▶ Prüfen Sie in jedem Einzelfall, welche Emails weitergeleitet werden.
- 
- ▶ Ermitteln Sie die ID der Email. Im Falle von infizierten Emails gibt AntiVir MailGate diese ID in seinen Meldungen und in seinen Email-Benachrichtigungen an den Postmaster an.
  - ▶ Geben Sie ein (ID steht dabei für die ID der betreffenden Email):  
`/usr/lib/AntiVir/avq --deliver=ID`  
↳ Die Email wird unabhängig vom Ergebnis des Virenskans weitergeleitet und aus der Queue gelöscht.



## 4.5 Vorgehen bei Auffinden eines Virus oder unerwünschten Programms

AntiVir MailGate hat bei richtiger Konfiguration alle wichtigen Aufgaben auf Ihrem Rechner bereits automatisch erledigt:

- Die infizierte Email wurde nicht weitergeleitet.
- Die infizierte Email wurde in das Verzeichnis `/var/spool/avmailgate/rejected` (oder das in der Datei `avmailgate.conf` festgelegte Verzeichnis) verschoben; d. h., dort liegen das data file (df-) und das control file (vf- oder mf-). Für weitere Informationen siehe [Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen](#) – Seite 50.
- Das data file enthält die Email, in der der Virus bzw. das unerwünschte Programm gefunden wurde. Diese kann nun entweder zusammen mit dem control file gelöscht oder durch Ausführen des Queue Manager Skripts `avq` weiterbehandelt werden.
- Je nach Konfiguration der Datei `avmailgate.conf` haben der Postmaster sowie Absender und/oder Empfänger der infizierten Email eine Warnung erhalten.
- Je nach Konfiguration der Datei `avmailgate.conf` wurde die infizierte Datei durch externe Programme oder Skripte weiterverarbeitet.

Die Gefahr einer weiteren Infektion ist damit gebannt.

Folgende Schritte sollten Sie auf jeden Fall durchführen:

- ▶ Versuchen Sie zu ermitteln, auf welche Weise die Infektion "eingeschleppt" wurde.
- ▶ Führen Sie gezielte Prüfungen an möglicherweise infizierten Datenträgern durch.
- ▶ Informieren Sie Kollegen, Vorgesetzte oder Geschäftspartner.
- ▶ Informieren Sie Ihren Systemverantwortlichen, Ihren Viren- oder Datenschutzbeauftragten.

### Verdächtige Dateien an H+BEDV Datentechnik GmbH schicken

- ▶ Senden Sie uns bitte Viren bzw. unerwünschte Programme, die von unseren Produkten noch nicht erkannt oder entfernt werden können, zu. Das Gleiche gilt für sonstige verdächtige Dateien. Senden Sie uns den Virus bzw. das unerwünschte Programm gepackt (gzip, WinZIP, PKZip, Arj) im Anhang einer Email an [virus@antivir.de](mailto:virus@antivir.de).



Verwenden Sie beim Packen das Passwort **virus**. Die Datei kann dann nicht von eventuellen Virensclannern in den Email-Gateways gelöscht werden.

---

## 5 Konfiguration

Um AntiVir MailGate optimal an Ihr System anzupassen, können Sie das Programm konfigurieren. Wenn Sie das Programm mit dem Skript `avinstall.pl` installiert haben, wurden Ihnen bereits Einstellungen vorgeschlagen, die für viele Fälle sinnvoll sind. Sie können jederzeit nachträglich diese Einstellungen ändern.

Dieses Kapitel führt Sie Schritt für Schritt in die Konfiguration ein. Es ist in folgende Abschnitte untergliedert:

- [Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen](#) – Seite 50
- [Konfigurieren der Datei `avmailgate.conf`](#) – Seite 51
- [Konfigurieren der Datei `avmailgate.acl`](#) – Seite 64
- [Virenspezifische Warnungen: Konfigurieren der Datei `avmailgate.warn`](#) – Seite 65
- [Konfigurieren der Vorlagen für Nachrichten](#) – Seite 66
- [Konfigurieren regelmäßiger Updates](#) – Seite 68
- [Konfigurieren der Update-Nachrichten](#) – Seite 71



Die Konfigurationsdateien werden beim Start des Programms eingelesen. Leerzeilen und Zeilen, die mit `#` beginnen, werden ignoriert.

Bei Lieferung der Software sind bereits Werte eingestellt, die für viele Anwendungen sinnvoll sind. Bei einigen Einstellungen mit einem vorgestellten `#` werden default-Werte angewendet. Durch Entfernen des `#` können die Werte geändert werden.

---

### 5.1 Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen

AntiVir MailGate sorgt dafür, dass eine infizierte Email gesondert abgelegt wird ("Quarantäne"). Zusätzlich erhalten – je nach Konfiguration – der Postmaster und/oder Absender und/oder Empfänger der Email eine Nachricht über das Auftreten des Virus bzw. unerwünschten Programms. Diese Parameter sind in der Datei `avmailgate.conf` einstellbar (siehe [Konfigurieren der Datei avmailgate.conf](#) – Seite 51).

Spool-  
Verzeichnisse

Das Spool-Verzeichnis (Standard: `/var/spool/avmailgate/`) ist unterteilt in drei weitere Verzeichnisse:

- **incoming:** enthält eingehende Emails, die noch geprüft werden müssen
- **outgoing:** enthält bereits geprüfte Emails, die weitergeleitet werden sollen
- **rejected:** enthält Emails, in denen ein Virus oder ein unerwünschtes Programm gefunden wurde oder die z. B. aufgrund von MIME-Fehlern als problematisch eingestuft wurden

Spool-  
Dateien

In diesen Verzeichnissen wird jede Email durch zwei Dateien repräsentiert:

- Datendatei (data file)
- Kontrolldatei (control file)

Die Datendatei wird im Dateinamen durch ein führendes `df-` und eine nachfolgende Datei-ID (z.B. `32557-0BE692EB`) gekennzeichnet. Die zugehörige Kontrolldatei wird durch die gleiche ID gekennzeichnet, die führenden Buchstaben im Dateinamen variieren, je nach Bearbeitungszustand der Email:

- **xf-:** Kontrolldatei wird gerade bearbeitet
- **qf-:** Email liegt für eine Prüfung auf Viren und unerwünschte Programme bereit
- **Qf-:** Email liegt für eine direkte Weiterleitung ohne Prüfung auf Viren und unerwünschte Programme bereit
- **vf-:** Email enthält einen Virus bzw. ein unerwünschtes Programm
- **mf-:** Email mit einem MIME-Problem

Beispiel

- Datendatei: `df-32557-0BE692EB`
- Zugehörige Kontrolldatei: `qf-32557-0BE692EB`

Bearbeitung der Spool-Dateien Wird ein Virus oder unerwünschtes Programm gefunden, liegen schließlich im Verzeichnis `/var/spool/avmailgate/rejected/`:

- df-Datei
- vf-Datei oder mf-Datei

Auf diese Dateien können externe Programme oder Skripte zugreifen, z. B. mit der `ExternalProgram`-Anweisung (siehe [Konfigurieren der Datei `avmailgate.conf`](#) – Seite 51).

Wird kein Virus oder unerwünschtes Programm gefunden, werden Daten- und Kontrolldatei nach der Überprüfung und Weiterleitung gelöscht.

## 5.2 Konfigurieren der Datei `avmailgate.conf`

Die Datei `avmailgate.conf` enthält zahlreiche Parameter für die Arbeit mit AntiVir MailGate. Wie in [Funktionsweise von AntiVir MailGate](#) – Seite 9 beschrieben, teilen sich die beiden Programme `avgated` und `avgatefd` die Arbeit.

- Vorgehen Konfiguration
- Editieren Sie `avmailgate.conf` entsprechend Ihren Wünschen.
  - Starten Sie MailGate neu, damit die neuen Einstellungen wirksam werden:

```
/usr/lib/AntiVir/avmailgate restart
```

Im Folgenden werden die Einträge in `avmailgate.conf` – thematisch zusammengefasst – kurz beschrieben. Diese Einträge beeinflussen nur das Verhalten von AntiVir MailGate und nicht die anderen Programme von AntiVir. Wie Sie diese Einstellungen über eine grafische Benutzeroberfläche komfortabel editieren können, erfahren Sie in [AntiVir MailGate über GUI konfigurieren](#) – Seite 79.

### Benutzer und Verzeichnisse festlegen (avgated und avgatefwd)

User, Group    **Benutzer/Gruppe:**

Benutzer und Gruppe, mit denen die MailGate-Prozesse arbeiten sollen (dies sollte nicht root sein).

```
User          uucp
Group         antivir
```

Wenn diese Einstellungen geändert werden, müssen die Zugriffsrechte auch für die betroffenen Verzeichnisse nachgezogen werden.

Postmaster    **Postmaster:**

Empfänger von Warnungen vor Viren bzw. unerwünschten Programmen sowie anderer Nachrichten:

```
Postmaster    postmaster
```

MyHostName    **Host-Name:**

FQDN (Fully Qualified Domain Name) des lokalen Hosts.

Wenn dies auskommentiert wurde, ist die Standardeinstellung der hostname, der von gethostname(2) zurückgegeben wird. Andernfalls ist localhost voreingestellt:

```
MyHostName    localhost
```

SpoolDir    **Spool-Verzeichnis:**

In den Unterverzeichnissen incoming, rejected und outgoing werden Emails während des Prozessablaufs abgelegt.

Das Spool-Verzeichnis muss dem unter User angegebenen Benutzer mit zugehöriger Gruppe gehören. Es darf nur für ihn zugänglich sein (mode=700).

```
SpoolDir      /var/spool/avmailgate
```

AntiVirDir    **AntiVir-Verzeichnis:**

Verzeichnis mit dem AntiVir Hauptprogramm, der Virusdefinitionsdatei antivir.vdf und der Lizenzdatei:

```
AntiVirDir    /usr/lib/AntiVir
```

## TemporaryDir **Temporäres Verzeichnis:**

In diesem Verzeichnis liegen die temporären Dateien (z. B. Email-Anhänge, die auf Viren bzw. unerwünschte Programme untersucht werden). Für ungepackte Anhänge wird entsprechend ausreichender Platz benötigt.

```
TemporaryDir      /var/tmp
```

oder

```
TemporaryDir      /tmp
```

## MatchMailAddressForLocal **Domänen-Namen prüfen:**

Mit dieser Option wird festgelegt, ob die Domänen-Namen der Empfängeradressen (RECIPIENT), der Absenderadressen (SENDER) oder beider Adressen (BOTH) auf die Einträge in dem `local:-`Abschnitt in der Datei `avmailgate.acl` geprüft werden sollen.

Nähere Informationen finden Sie im Kapitel [Konfigurieren der Datei av-mailgate.acl](#) – Seite 64.

```
MatchMailAddressForLocal  RECIPIENT
```

## SMTPBanner **SMTP-Begrüßungstext:**

Meldungszeile, die MailGate an den Mailserver ausgibt. Sie können den Text editieren, z. B. wenn die Art der eingesetzten Virenschutz-Software nicht bekannt gegeben werden soll.

```
SMTPBanner        "AntiVir MailGate"
```

## PidDir **PID-Verzeichnis:**

In diesem Verzeichnis werden die PID-Dateien für die MailGate-Hauptprozesse gespeichert (`avgated` und `avgatefwd`).

```
PidDir             /var/tmp
```

oder

```
PidDir             /tmp
```

## LogFile **Logdatei:**

Die Angabe muss den vollständigen Pfad zu einer separaten Logdatei enthalten. Neben den Einträgen in dieser Logdatei werden auch Einträge an den `syslog` gesendet.

Wenn `LogFile` auf `NO` gesetzt ist, wird keine separate Logdatei verwendet. Es werden aber Einträge an den `syslog` gesendet.

```
LogFile            /var/log/avmailgate.log
```

– ODER –

```
LogFile            NO
```

### Verbindungen konfigurieren (avgated)

Listen Address	<b>IP-Adresse:</b> Schnittstelle und Port, an denen der SMTP-Dämon lauscht. AntiVir MailGate lauscht an allen Netzwerkkarten (bei 0.0.0.0) oder man kann eine IP-Adresse für eine einzelne Netzwerkkarte angeben. Wenn Sie unsicher über die Einstellung sind, lassen Sie die Standardeinstellung unverändert:  ListenAddress 0.0.0.0 port 25
MaxIncoming Connections	<b>Maximale Anzahl gleichzeitig eingehender Verbindungen:</b> Begrenzt die Anzahl gleichzeitiger Verbindungen von der Remote-Site. Sie können z. B. angeben, dass maximal 100 Emails gleichzeitig eingehen können. Der Wert 0 (Standardeinstellung) schaltet diese Option aus; d. h. es können unbegrenzt viele Emails passieren.  MaxIncomingConnections 0
SMTP Timeout	<b>SMTP Timeout:</b> Definiert die maximale Dauer der SMTP-Connection in Sekunden.  SMTPTimeout 300
MaxMessage Size	<b>Maximale Größe einer Email:</b> Wenn ein Wert >0 Bytes eingestellt ist, werden nur Emails bis zu dieser Größe überprüft. Größere Emails werden abgewiesen.  Wenn der Wert 0 eingestellt ist, werden Emails unabhängig von ihrer Größe überprüft.  MaxMessageSize 0
MinFree Blocks	<b>Minimum an freien Blöcken auf Dateisystem:</b> AntiVir MailGate blockt eingehende Verbindungen ab, wenn die Anzahl der freien Blöcke im Dateisystem (also der Speicherplatz auf der Festplatte) kleiner als der angegebene Wert ist.  MinFreeBlocks 100
Max Recipients PerMessage	<b>Maximale Anzahl an Empfängern pro Email:</b> Definiert die maximale Anzahl der Empfänger, die eine Nachricht erhalten können. Der Wert 0 schaltet diese Option aus.  MaxRecipientsPerMessage 100



RefuseEmpty  
MailFrom

## Email mit leerem Absender akzeptieren:

Es ist möglich, Emails mit leerem Absender abzulehnen. Die Standardeinstellung ist NO, d. h. der SMTP-Server akzeptiert alle eingehenden Emails. Diese Einstellung sollte nicht geändert werden.

RefuseEmptyMailFrom NO



RFC2821, RFC821 und RFC2505 empfehlen, dass ein SMTP-Server alle Emails (auch ohne Absenderadresse) annehmen muss. Es wird empfohlen, die Standardeinstellung des Parameters RefuseEmptyMailFrom nicht zu ändern.

## Behandlung von Email-Adressen definieren (avgated)

AllowSource  
Routing

### Source-Routing zulassen:

Source routing wird durch folgende Adress-Syntax erreicht:

@ONE, @TWO:JOE@THREE

Mit dieser Adresse wird festgelegt, welchen Weg eine Email nehmen soll: Sie soll über ONE und TWO und schliesslich an JOE auf dem Host THREE ausgeliefert werden.

Mit dieser Option wird festgelegt, ob alles ausser JOE@THREE entfernt (NO) oder ob die Adresse beibehalten werden soll (YES).

AllowSourceRouting NO

InEnvelope  
Addresses  
BangIs

### Ausrufezeichen in der Empfängeradresse:

Wenn REFUSED eingestellt und ein "!" in der Empfängeradresse ist, wird die Meldung zurückgewiesen.

Wenn IGNORED eingestellt ist, wird ein "!" wie ein normales Zeichen der Empfängeradresse behandelt.

Wenn INTERPRETED eingestellt ist, wird die Empfängeradresse in eine RFC821-gemäße Standardform umgewandelt. Z. B. wird die Adresse

hostA!hostB!hostC!user

umgewandelt in

hostA, @hostB:user@hostC

Wenn Source-Routing erlaubt ist, wird die Email an hostA gesendet, andernfalls an hostC.

InEnvelopeAddressesBangIs REFUSED

InEnvelope  
Addresses  
PercentIs

### **Prozentzeichen in der Empfängeradresse:**

Wenn `REFUSED` eingestellt und ein "%" in der Empfängeradresse ist, wird die Meldung zurückgewiesen.

Wenn `IGNORED` eingestellt ist, wird ein "%" wie ein normales Zeichen der Empfängeradresse behandelt.

Wenn `INTERPRETED` eingestellt ist, wird die Empfängeradresse in eine RFC821-gemäße Standardform umgewandelt. Z. B. wird die Adresse

```
user%hostC%hostB@hostA
```

umgewandelt in

```
@hostA,@hostB:user@hostC
```

Wenn Source-Routing erlaubt ist, wird die Email an hostA gesendet, andernfalls an hostC.

```
InEnvelopeAddressesPercentIs    REFUSED
```

AcceptLoose  
DomainName

### **Domänen-Syntax von Emails prüfen:**

Ein Domänen-Name darf nur aus folgenden Zeichen bestehen: `[-.0-9A-Za-z]`.

Der Parameter `AcceptLooseDomainName` lässt auch nicht korrekte Domänen-Namen zu.

Wenn `NO` eingestellt und der Domänen-Name für die Zustellung der Meldung nicht korrekt ist (abhängig vom Source-Routing), wird die Meldung zurückgewiesen.

Wenn `YES` eingestellt ist, wird der Domänen-Name nicht geprüft; d. h., auch Emails mit nicht korrektem Domänen-Namen werden weitergeleitet.

```
AcceptLooseDomainName    NO
```

AddressFilter

### **Email-Adressen filtern:**

Mit dieser Option wird der Adressfilter aktiviert/deaktiviert. Standardeinstellung ist `NO`, d. h., dass bei der Standardinstallation kein Adressfilter verwendet wird.

```
AddressFilter    YES
```

Um den Adressfilter nutzen zu können, müssen folgende Dateien vorhanden sein:

```
/etc/avmailgate.ignore
```

und

```
/etc/avmailgate.scan
```

Diese Dateien enthalten zeilenweise Email-Adressen und optional die Flags S/s (Senderadresse) und/oder R/r (Empfängeradresse). Die angegebenen Email-Adressen werden nur über das SMTP-Protokoll (MAIL FROM und RCPT TO) geprüft. Die Email-Adressen in den Email-Headern werden nicht beachtet.

Die Listen werden auf Übereinstimmung geprüft. Zuerst wird die Liste geprüft, die an erster Stelle im FilterTableOrder steht. Sobald eine Übereinstimmung vorliegt, wird die weitere Prüfung der Listen abgebrochen und die konfigurierte Aktion ausgeführt.

Je nach Ergebnis werden folgende Aktionen ausgelöst:

- Liegt keine Übereinstimmung mit der ersten Liste vor, wird die nächste Liste geprüft.
- Liegt auch hier keine Übereinstimmung vor, wird die Email gescannt.
- Liegt eine Übereinstimmung mit der ignore-Liste vor, wird die Email nicht gescannt.
- Liegt eine Übereinstimmung mit der scan-Liste vor, wird die Email gescannt.

Die Email-Adressen müssen Perl-kompatible reguläre Ausdrücke sein, z. B.:

```
/abc/  
/^abc/  
/xyz/i  
/^abc@def\.tld/
```

### Beispiel:

/etc/avmailgate.ignore enthält folgende Zeilen:

```
/^jemand@irgendwo\.tld$/ SR  
/^virus@firma/ R  
/^abc@def.*\.tld/i
```

Ist die Adresse des Senders oder Empfängers jemand@irgendwo.tld, wird die Email nicht gescannt.

Ist die Adresse des Empfängers virus@firma\*, wird die Email nicht gescannt. Die Angabe des Flags R ist in diesem Fall optional:  
/^virus@firma/ R ist gleichbedeutend mit /^virus@firma/.

Beim Starten von AntiVir MailGate wird im maillog angegeben, ob der Adressfilter aktiv ist oder nicht:

```
addressfilter is active  
table order is: ignore,scan
```

oder

```
addressfilter is not active
```

Filter  
TableOrder

### **Suchreihenfolge der Filtertabelle:**

Die Option ist nur bei aktiviertem Adressfilter (AddressFilter YES) von Bedeutung. Mögliche Parameter sind:

`scan, ignore`

oder

`ignore, scan`

## **Emails weiterleiten (avgatefwd)**

PollPeriod

### **Warteschlange überprüfen:**

Legt das Zeitintervall in Sekunden fest, wann avgatefwd die Warteschlange nach neuen Emails durchsuchen soll, um sie auf Viren bzw. unerwünschte Programme zu prüfen.

`PollPeriod 60`

ScanTimeout

### **Maximale Zeit zum Scannen einer Email:**

Definiert die maximale Dauer des Email-Scans in Sekunden.

`ScanTimeout 300`

Max  
Forwarders

### **Maximale Anzahl der Forwarder:**

Maximale Anzahl der Weiterleitungsprozesse (avgatefwd), die gleichzeitig laufen können. Der Wert ist abhängig von der Leistungsfähigkeit Ihres Email-Systems und der Qualität Ihrer Netzwerkverbindung (Standardeinstellung: 10).

`MaxForwarders 10`

ForwardTo

### **Forwarder:**

Definiert, wie die Email weitergeleitet werden soll, Standardeinstellung ist das Versenden per sendmail.

`ForwardTo /usr/lib/sendmail -oem -oi`

Die Email kann jedoch auch per SMTP weitergeleitet werden:

`ForwardTo SMTP localhost port 825`

oder

`localhost port smtp-backdoor`

Max  
Attachments

### **Maximale Anzahl an Email-Anhängen (MIME):**

Definiert die maximale Anzahl der zu scannenden Anhänge pro MIME-Email.

`MaxAttachments 100`

**Block Suspicious Mime** **Verdächtige Emails blocken (MIME):**  
 Blockt die Weiterleitung verdächtiger MIME-Emails. Eine MIME-Email wird als verdächtig eingestuft, wenn die maximale Zahl von Anhängen erreicht ist (Standardeinstellung: NO).

BlockSuspiciousMime NO

**Block Fragmented Message** **Fragmentierte Emails blocken:**  
 Blockt Emails, die fragmentiert (mehrteilig) zugestellt werden. Weitere Informationen siehe "Message Fragmentation and Reassembly", RFC 2046, <http://www.faqs.org/rfcs/rfc2046.html>, Abschnitt 5.2.2.1).

BlockFragmentedMessage NO

**ForwardAll EmailAs MIME** **Emails immer als MIME-Emails weiterleiten:**  
 Emails, die nicht als MIME-Emails ankommen, können zu MIME-Emails umgeschrieben werden. Sie bekommen einen MIME-Header, mit Content-Type: text/plain, Content-Disposition: inline und einem Content-Encoding: 7 bit oder 8 bit. Das "Encoding" hängt von der ursprünglichen Email ab.

Wenn NO eingestellt ist, werden eingehende Nicht-MIME-Emails ohne Bearbeitung weitergeleitet.

Wenn YES eingestellt ist, werden eingehende Nicht-MIME-Emails umgeschrieben in MIME-Emails.

ForwardAllEmailAsMIME NO

## Nachrichten senden (avgatefwd)

Zusätzlich zur Konfiguration über avmailgate.conf ist eine Konfiguration über avmailgate.warn möglich (siehe [Virenspezifische Warnungen: Konfigurieren der Datei avmailgate.warn](#) – Seite 65).

**Expose Recipient Alerts** **Warnungen an Empfänger betroffener Emails senden:**  
 Es können Warnungen vor Viren bzw. unerwünschten Programmen an die Empfänger gesendet werden. Folgende Möglichkeiten gibt es:

- **NO:** Es werden keine Warnungen an die Empfänger gesendet.
- **LOCAL:** Warnungen werden nur gesendet, wenn der Empfänger ein lokaler Benutzer Ihrer Domäne ist. Dies legen Sie in der Datei avmailgate.acl mit der Option local fest.
- **YES:** Es werden immer Warnungen an die Empfänger gesendet.

ExposeRecipientAlerts LOCAL

Expose  
SenderAlerts

### **Warnungen an Absender betroffener Emails senden:**

Es können Warnungen vor Viren bzw. unerwünschten Programmen an den Absender gesendet werden. Folgende Möglichkeiten gibt es:

- **NO:** Es wird keine Warnung an den Absender der betroffenen Email gesendet.
- **LOCAL:** Eine Warnung wird nur gesendet, wenn der Absender ein lokaler Benutzer Ihrer Domäne ist. Dies legen Sie in der Datei `avmailgate.acl` mit der Option `local` fest.
- **YES:** Es wird immer eine Warnung an den Absender der betroffenen Email gesendet.

```
ExposeSenderAlerts    LOCAL
```

Expose  
Postmaster  
Alerts

### **Warnungen an Postmaster senden:**

Sendet Warnungen vor Viren bzw. unerwünschten Programmen an den Postmaster.

```
ExposePostmasterAlerts    YES
```

NotifyEnd  
OfLicense

### **Über ablaufende Lizenz informieren:**

Sendet eine Meldung an den postmaster, wann die Lizenz von AntiVir abläuft (Angabe in Tagen). Die Angabe 0 bedeutet keine Meldung.

```
NotifyEndOfLicense    10
```

AlertsUser

### **Absender von Warnungen:**

Benutzername oder Email-Adresse des Absenders von Warnungen (wenn ein Virus bzw. unerwünschtes Programm in einer Email gefunden wurde):

```
AlertsUser            AvMailGate
```

oder

```
AlertsUser            AvMailGate@mailserver.mydomain.tld
```

Bounce  
MessageUser

### **Benutzername für Fehler-Emails:**

Der Absender von Fehlermeldungen, wenn eine Email nicht durch den MTA ausgeliefert werden konnte, ist der hier angegebene Name.

```
BounceMessageUser    MAILER-DAEMON
```

Bounce  
Message  
SizeBody

### **Größe bei Fehler-Emails (Mailbody):**

Gibt an, wieviele Bytes des original Mailbody mit der bounce mail zurückgeschickt werden sollen. Die Angabe 0 bedeutet kein Limit.

```
BounceMessageSizeBody    0
```

Bounce Message SizeHeader **Größe bei Fehler-E-mails (Mailheader):**  
 Gibt an, wieviele Bytes des original Mailheader mit der bounce mail zurückgeschickt werden sollen. Die Angabe 0 bedeutet kein Limit.  
 BounceMessageSizeHeader 0

## Nachricht in weitergeleitete E-mails einfügen (avgatefwd)

Mit den folgenden beiden Parametern können Sie Status-Informationen in eine weitergeleitete Email einfügen.

AddStatus InBody **Status-Benachrichtigung in Email:**  
 Wenn NO eingestellt ist, wird in die weitergeleitete Email keine Nachricht eingefügt.  
 Wenn YES eingestellt ist:

- Einfache RFC822-Email (keine MIME-Email): Nachricht wird an den Anfang der Email eingefügt.
- MIME-Email: Geprüfte Email als eine neue MIME multipart/mixed Email weiterleiten, mit einem Textabschnitt, der die Mitteilung über den Status beinhaltet, und einem zweiten RFC822-Abschnitt, der die gesamte Original-Email enthält. Die meisten Header vom Original werden in die weitergeleitete Nachricht kopiert.
- Wenn im Template-Verzeichnis eine Datei body-state existiert, wird der darin enthaltene benutzerdefinierte Text in die Email eingefügt (siehe [Konfigurieren der Vorlagen für Nachrichten](#) – Seite 66).

AddStatusInBody NO

AddXHeader **X-Header hinzufügen:**  
 Wenn YES eingestellt ist, wird der gescannten Email folgende Headerzeile hinzugefügt: **X-AntiVirus: checked by AntiVir MailGate...**  
 Der Text ist nicht modifizierbar.

AddXHeader YES

AddReceived ByHeader **Received by-Header hinzufügen:**  
 Wenn YES eingestellt ist, erhält die gescannte Email einen Vermerk im Header, wann sie eingegangen ist.

AddReceivedByHeader YES

**Add Precedence Header**    **Precedence-Header hinzufügen:**

Diese Option ist nur in der Professional Edition verfügbar. Wenn **YES** eingestellt ist, erhält die beim Fund eines Virus bzw. unerwünschten Programms versandte Email den Vermerk **Precedence: junk**. Programme, die auf eingegangene Emails automatisch antworten (z. B.: vacation), reagieren dann nicht auf diese Benachrichtigungs-Email. Der Eintrag **YES** oder **NO** kann durch einen eigenen Text ersetzt werden.

`AddPrecedenceHeader`    `NO`

**AddHeaderToNotice**    **Email-Header für Postmaster hinzufügen:**

Sie können den Header der verdächtigen Email in die Benachrichtigungs-Email an den Postmaster einfügen. Mögliche Einstellungen sind **YES** oder **NO**.

`AddHeaderToNotice`    `NO`

**UseProxy**    **Scans optimieren:**

Scans werden mit der Proxy-Option in SAVAPI effektiver ausgeführt, wenn sie einen festgelegten Pool an AntiVir-Scannern verwenden. Da dieser Pool den Durchsatz erhöht, muss die Größe des Pools sehr genau bestimmt werden: Zu viele Scanner verbrauchen zu viel Ressourcen, ohne die Leistung zu steigern, zu wenige Scanner führen dazu, dass die SAVAPI-Anwendungen unnötig lange warten. Mögliche Einstellungen sind **YES** oder **NO**.

`UseProxy`    `NO`

**Proxy Scanners**    **Anzahl der AntiVir-Scanner festlegen:**

Anzahl der AntiVir-Scanner im Pool (siehe auch `UseProxy`).

`ProxyScanners`    `8`

**Proxy Connections**    **Anzahl der gleichzeitigen Verbindungen zum Proxy festlegen:**

Anzahl der maximal zulässigen, gleichzeitigen Verbindungen zwischen AntiVir MailGate und Scanner-Pool.

`ProxyConnections`    `32`

### Dateien in angehängten Archiven scannen (avgatefwd)

**ScanIn Archive**    **Archive durchsuchen:**

Wenn **NO** eingestellt ist, werden Archive nicht auf Viren bzw. unerwünschte Programme durchsucht.

Wenn **YES** eingestellt ist, werden alle Dateien in Archiven dekomprimiert und durchsucht – abhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`.

`ScanInArchive`    `YES`



Archive  
MaxSize**Maximale Größe entpackter Dateien:**

Es gibt komprimierte Dateien, die keinen sinnvollen Inhalt haben, aber bewusst so angelegt sind, dass sie sich auf "unsinnige Größe" aufblähen, um den Rechner lahm zu legen. Dieser Parameter schützt vor dem Entpacken solcher Archiv-Dateien.

Wenn der Wert 0 Bytes eingestellt ist, werden alle Dateien in Archiven entpackt – unabhängig von ihrer Größe.

Wenn ein Wert >0 Bytes eingestellt ist, werden nur die Dateien durchsucht, die im entpackten Zustand nicht größer als dieser Wert sind.

```
ArchiveMaxSize      0
```

ArchiveMax  
Recursion**Maximale Rekursionstiefe bei Archiven:**

Wenn der Wert 0 eingestellt ist, werden rekursive (verschachtelte) Archive vollständig entpackt – unabhängig von der Rekursionstiefe.

Wenn ein Wert >0 eingestellt ist, werden Archive nur bis zu der angegebenen Rekursionstiefe entpackt. Hierdurch lässt sich Zeit sparen.

```
ArchiveMaxRecursion 5
```

ArchiveMax  
Ratio**"Mailbomben" blocken:**

Blockt so genannte "Mailbomben" mit einer sehr hohen Kompressionsdichte. Sie können angeben, bis zu welchem maximalen Verhältnis zwischen gepackter und entpackter Dateigröße Dateien aus Archiven entpackt werden dürfen.

Der Wert 0 schaltet diese Option aus. Diese Einstellung wird **nicht** empfohlen. Die Standardeinstellung ist 150.

```
ArchiveMaxRatio      150
```

Block  
Suspicious  
Archive**Emails mit verdächtigen Archiven blocken:**

Wenn YES eingestellt ist, können Emails mit verdächtigen Archiven abgewiesen werden – abhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio.

Wenn NO eingestellt ist, werden Emails unabhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio zugestellt.

```
BlockSuspiciousArchive NO
```

Block  
Encrypted  
Archive**Emails mit Passwort-geschützten Archiven blockieren:**

Wenn YES eingestellt ist, werden Emails abgewiesen, wenn sie Passwort-geschützte Dateien in einem Archiv enthalten.

Wenn NO eingestellt ist, werden Emails auch zugestellt, wenn sie Passwort-geschützte Dateien in einem Archiv enthalten.

```
BlockEncryptedArchive NO
```

### Externes Programm ausführen (avgatefwd)

**External Program**    **Externes Programm oder Script bei Fund von Viren bzw. unerwünschten Programmen ausführen:**

Ruft ein externes Programm oder ein Skript auf, wenn ein Virus bzw. unerwünschtes Programm gefunden wurde. Der Parameter ist die ID der zurückgewiesenen Email (siehe [Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen](#) – Seite 50).

```
ExternalProgram     /dir/my_own_script
```

### Unterstützung durch GUI aktivieren (avgatefwd)

**GUISupport**    **Unterstützung durch GUI aktivieren:**  
Dieser Eintrag muss aktiviert sein, damit MailGate mit der GUI kommunizieren kann. Folgende Parameter müssen eingetragen sein:

```
GuiSupport         YES
GuiCAFile          /usr/lib/AntiVir/gui/cert/cacert.pem
GuiCertFile        /usr/lib/AntiVir/gui/cert/server.pem
GuiCertPass        antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht die GUI nicht zur Verfügung.

## 5.3 Konfigurieren der Datei avmailgate.acl

In der Datei avmailgate.acl wird anhand der Schlüsselwörter local und relay festgelegt, welchen Rechnern das Verschicken von Emails über AntiVir MailGate erlaubt wird. Dies wird über die Absender- und/oder Empfänger-Domäne bzw. die IP-Adresse festgelegt.

- Legen Sie fest, welche Hosts und/oder Domänen lokal sind, z. B.

```
local: localhost
```

```
local: hbedv.com antivir.de
```

- Legen Sie fest, welche Hosts und Netzwerke Emails verschicken dürfen, z. B.

```
relay: 127.0.0.1/8 192.168.0.0/16
```

**IP-Adressen**    Sie können IP-Adressen auf verschiedene Art und Weise angeben:

```
192.168.0.0/16 oder 192.168
```

haben die gleiche Bedeutung. /16 bedeutet 16 bit und bezeichnet die ersten beiden Zahlen der IP-Adresse. D. h., es sind alle IP-Adressen erlaubt, die mit 192.168 beginnen.

## 5.4 Virenspezifische Warnungen: Konfigurieren der Datei avmailgate.warn

Optional können Sie eine weitere Datei `/etc/avmailgate.warn` anlegen. Diese Datei spezifiziert über `avmailgate.conf` hinaus das Versenden von Emails mit Warnmeldungen an Absender, Empfänger und Postmaster.

Eine Zeile dieser Datei besteht aus zwei Einträgen: Der erste Eintrag ist der Name des gefundenen Virus bzw. unerwünschten Programms. Dieser Eintrag kann Wildcards enthalten. Der zweite Eintrag besteht aus einem oder mehreren der folgenden Buchstaben:

- S: für Absender
- R: für Empfänger
- P: für Postmaster

Beispiel Die Zeile

```
/klez/ RP
```

weist AntiVir MailGate an, im Falle eines gefundenen Virus mit dem Namenbestandteil **Klez** eine Warn-Email an den Empfänger und den Postmaster zu verschicken.



Die Einstellungen in `avmailgate.warn` setzen für die spezifizierten Viren und unerwünschten Programme die Einstellungen in `avmailgate.conf` außer Kraft.

### 5.5 Konfigurieren der Vorlagen für Nachrichten

Wenn Sie eine Lizenzdatei verwenden, haben Sie die Möglichkeit, eigene Meldungstexte für die Emails festzulegen, die beim Fund von Viren bzw. unerwünschten Programmen sowie sonstigen verdächtigen Dateien gesendet werden.

- ▶ Legen Sie das folgende Verzeichnis an:  
`mkdir /usr/lib/AntiVir/templates`
- ▶ Kopieren Sie die Beispiel-Vorlagen in der gewünschten Sprache aus dem Vorlagen-Verzeichnis `/tmp/antivir-mailgate-prof-<version>/templates/Sprache/` in das Verzeichnis `/usr/lib/AntiVir/templates`.
- ▶ Legen Sie die Zugriffsrechte fest:  
`chown -R uucp:antivir/usr/lib/AntiVir/templates`
- ▶ Wechseln Sie in das Verzeichnis `/usr/lib/AntiVir/templates`. Dieses Verzeichnis enthält folgende Dateien:  
patho-administrator  
patho-recipient  
patho-sender  
virus-administrator  
virus-recipient  
virus-sender
- ▶ Fügen Sie in die o. g. Dateien Ihren eigenen Meldungstext ein. Beachten Sie den Aufbau der Dateien:
  - In der ersten Zeile steht der Betreff der Email.
  - Anschließend folgt eine Leerzeile (neue Zeile).
  - Anschließend folgt der Text der Email.

Schlüsselwörter Die virus-\* und patho\*-Dateien können folgende Schlüsselwörter enthalten, die jeweils durch den entsprechenden Text ersetzt werden.

Schlüsselwort	Ersetzungstext
LICENSE	Lizenztext (ein bis zwei Zeilen).
SENDER	Email-Adresse des Absenders der infizierten Email.
VIRUSES	Liste der Viren bzw. unerwünschten Programme, die in der infizierten Email gefunden wurden. Jede Zeile enthält den Namen eines Virus bzw. unerwünschten Programms, wobei Präfix und Postfix in jeder Zeile wiederholt werden.
REASON	Angabe des Grundes, aus dem die Email nicht gescannt werden konnte (kurzer Satz).
ADVICE	Vorschlag, wie der Absender das Problem lösen kann (siehe REASON) (ungefähr eine Zeile)
QUEUEID	ID der Email in der AntiVir MailGate-Warteschlange
SUBJECT	Betreffzeile der infizierten Email

Beispiel Beispiel für eine Datei virus-recipient:

```
SUBJECT: AntiVir ALARM [Ihre Email: "SUBJECT"]
```

```
*****AntiVir ALARM*****
*****
```

```
LICENSE
```

```
*****
```

```
AntiVir hat Folgendes in der Email, die von Ihrer Adresse aus versandt wurde, entdeckt:
```

```
VIRUSES
```

```
Die Email wurde nicht zugestellt!
```

```
Diese Email wurde nicht ausgeliefert, sondern auf Ihrem Server isoliert. Prüfen Sie bitte Ihr System unverzüglich auf eventuellen Befall mit Viren.
```

```
Entfernen Sie vorhandene Viren, bevor Sie weitere Emails mit Dateianhängen versenden.
```

### 5.6 Konfigurieren regelmäßiger Updates

Die Leistungsfähigkeit und Wirksamkeit einer Virensoftware steht und fällt mit ihrer Aktualität. Deshalb bietet AntiVir MailGate die Möglichkeit, jederzeit Updates über HTTP vom AntiVir-Webserver zu laden – manuell oder automatisiert in regelmäßigen Abständen.

Bei diesen Updates werden die Bestandteile von AntiVir MailGate, die den Schutz vor Viren und unerwünschten Programmen sicherstellen (vdf-Datei und Scan Engine), auf den neuesten Stand gebracht.

Wir empfehlen, AntiVir MailGate so zu konfigurieren, dass das Programm in bestimmten Zeitabständen automatisch auf der H+BEDV-Webseite nach Updates sucht.

Wie Sie Informationen über Updates erhalten, lesen Sie im Kapitel [Konfigurieren der Update-Nachrichten](#) – Seite 71.

#### Internet-Zugang für Updates konfigurieren

- ✓ Stellen Sie sicher, dass Ihr Internetzugang funktioniert. In den meisten Fällen wird der Internetzugang bereits konfiguriert sein. Ansonsten entnehmen Sie die notwendigen Informationen Ihrer UNIX-Dokumentation.

**Proxy-Server** Falls Sie über einen HTTP-Proxy-Server mit dem Internet verbunden sind, müssen Sie die entsprechenden Einstellungen in der Konfigurationsdatei `antivir.conf` vornehmen. Es sind keine Standardeinstellungen vorgesehen.

- ▶ Öffnen Sie die Datei `/etc/antivir.conf`.
- ▶ Geben Sie den Namen des Proxy-Servers ein, z. B.:  
`HTTPProxyServer proxy.domain.com`
- ▶ Geben Sie den Port des Proxy-Servers ein, z. B.:  
`HTTPProxyPort 8080`

Wenn Username und Passwort erforderlich sind:

- ▶ Geben Sie Username und Passwort ein, z. B.:  
`HTTPProxyUsername username`  
`HTTPProxyPassword password`

Der Internet-Zugang für Updates ist konfiguriert.

### Automatische Updates über Cron-Dämon steuern

Regelmäßige Updates werden über den Cron-Dämon gesteuert. Die Einstellung in der Datei `/etc/crontab` wurde bereits vorgenommen, wenn Sie AntiVir MailGate mit dem Installationsskript `avinstall.pl` installiert haben und hierbei die Frage, ob der AntiVir Updater installiert werden soll, mit `yes` beantwortet haben.

Nähere Informationen über den Cron-Dämon entnehmen Sie Ihrer UNIX-Dokumentation.

- Nehmen Sie den entsprechenden Eintrag in der Datei `/etc/crontab` vor. Die Option `-q` bewirkt, dass keine Meldungen ausgegeben werden.

**Beispiel:** Fügen Sie für ein stündliches Update um `*:23` Uhr folgende Zeile ein:

```
23 * * * * root /usr/lib/AntiVir/antivir --update -q
```

- Starten Sie den Update-Vorgang, um die Einstellungen zu testen:

```
/usr/lib/AntiVir/antivir --update
```

- ↳ Bei erfolgreicher Ausführung liegt in der Logdatei `/var/log/antivir.log` eine Nachricht.

Wenn kein neues Update verfügbar ist, erhalten Sie folgende Nachricht (Beispiel):

```
checking for updates

06.18.00.07 <=> [vdf,loaded]
06.18.00.02 <=> [engine,running]
02.00.06.13 <=> [program,running]
```

### Authentizität der Updates durch GnuPG sicherstellen

GnuPG ist eine kostenlose Alternative zum Verschlüsselungsprogramm PGP (Pretty Good Privacy). Mit GnuPG kann die Authentizität der Updates von AntiVir MailGate sichergestellt werden. Die Verwendung von GnuPG wird sehr empfohlen.



Allerdings setzt die Verwendung vertiefte Kenntnisse von UNIX und GnuPG voraus. Bei fehlerhafter Konfiguration besteht ansonsten die Gefahr, dass AntiVir MailGate nicht mehr aktualisiert wird.

Weitere Informationen zu GnuPG erhalten Sie über <http://www.gnupg.org>

Führen Sie folgende Schritte durch, um die Unterstützung von GnuPG zu aktivieren:

- ▶ Laden Sie GnuPG von der GnuPG-Webseite <http://www.gnupg.org>. Hier erhalten Sie auch ein Handbuch mit weiterführenden Informationen zu PGP und dessen Anwendungsmöglichkeiten.
- ▶ Erzeugen Sie Ihren eigenen PGP-Schlüssel, wie in der GnuPG-Dokumentation beschrieben.
- ▶ Fügen Sie den öffentlichen AntiVir-PGP-Schlüssel zu Ihrem Schlüsselbund hinzu:

```
gpg --import antivir.gpg
```

- ▶ Fordern Sie den Fingerabdruck des Schlüssels an, um sicherzustellen, dass es tatsächlich der öffentliche AntiVir-PGP-Schlüssel ist:

```
gpg --fingerprint support@antivir.de
```

↳ Der 40-stellige Fingerabdruck wird ausgegeben.

- ▶ Stellen Sie sicher, dass der ausgegebene Fingerabdruck mit dem Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels übereinstimmt. Der Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels wird auf der AntiVir-Webseite (<http://www.antivir.de>) angezeigt.

- ▶ Unterschreiben Sie den öffentlichen AntiVir-PGP-Schlüssel, um seine Gültigkeit zu beglaubigen:

```
gpg --sign-key support@antivir.de
```

- ▶ Wechseln Sie in das Unterverzeichnis /bin Ihres AntiVir-Installationsverzeichnisses, also z. B.:

```
cd /tmp/AntiVir/bin
```

↳ In diesem Verzeichnis liegen die Dateien antivir und antivir.asc.

- ▶ Prüfen Sie die Unterschrift mit

```
gpg --verify antivir.asc antivir
```

↳ Wenn Sie keine Fehlermeldungen erhalten, ist GnuPG bereit für Updates von AntiVir MailGate.

- ▶ Aktivieren Sie GnuPG für AntiVir MailGate. Tragen Sie hierfür in der Konfigurationsdatei /etc/antivir.conf im Eintrag GnuPGBinary den vollen Pfad zur GnuPG-Binärdatei ein, z. B.:

```
GnuPGBinary          /usr/local/bin/gpg
```

- ▶ Starten Sie den antivirupdater neu, um die geänderten Einstellungen in antivir.conf wirksam werden zu lassen:

```
/usr/lib/AntiVir/antivirupdater restart
```

Die Authentizität der Updates wird ab jetzt durch GnuPG sichergestellt.



## 5.7 Konfigurieren der Update-Nachrichten

Die hier beschriebenen Einstellungen für Nachrichten über Updates des Programms werden in der Konfigurationsdatei `/etc/antivir.conf` vorgenommen.

- ▶ Öffnen Sie die Datei `/etc/antivir.conf`.
- ▶ Nehmen Sie die gewünschten Einstellungen vor.

### Email-Versand bei Updates anpassen

Alle Nachrichten über Updates von AntiVir MailGate werden an die angegebene Email-Adresse geschickt.

EmailTo ▶ Geben Sie die Email-Adresse ein, z. B.  
                     EmailTo                      root@localhost

### Syslog-Nachrichten spezifizieren

Für alle wichtigen Operationen gibt AntiVir Nachrichten an den syslog-Dämon. Sie können spezifizieren, welche Facility und Priorität diesen Nachrichten mitgegeben wird.



Wenn Sie keine Erfahrung mit dem syslog-Dämon haben, sollten Sie die voreingestellten Werte nicht ändern. Nähere Informationen zum syslog-Dämon entnehmen Sie Ihrer UNIX-Dokumentation.

Syslog Facility ▶ Geben Sie eine neue Facility ein oder wählen Sie die Standardeinstellung:  
                     SyslogFacility              user

Syslog Priority ▶ Geben Sie eine neue Priorität ein oder wählen Sie die Standardeinstellung:  
                     SyslogPriority              notice

### Logdatei anpassen

Zusätzlich zu syslog können Nachrichten über Updates in eine separate Logdatei geschrieben werden. Für diesen Parameter gibt es keine Standardeinstellung.

- ▶ Geben Sie Name und vollen Pfad der Logdatei ein, z. B.  
                     /var/log/antivir.log



## 6 Grafische Benutzeroberfläche (GUI)

### 6.1 Übersicht

Die grafische Benutzeroberfläche (GUI) unterstützt Sie bei der Bedienung und Konfiguration von AntiVir MailGate und stellt den laufenden Überwachungsprozess grafisch dar. AntiVir MailGate ist aber auch ohne GUI voll funktionsfähig und vollständig konfigurierbar. Die GUI ist eine programmunabhängige Applikation. D. h., sie kann gestartet und gestoppt werden, ohne dass AntiVir MailGate beeinflusst wird.

Für die GUI benötigen Sie Java 1.4.0 oder höher.

**Rechte** Mit GUI kann man das Programm als normaler Benutzer steuern, es sind keine root-Rechte erforderlich.

Allerdings muss der Benutzer in der "antivir"-Gruppe sein, die bei der Installation angelegt wird.

► Dafür geben Sie ein (als root):

```
/usr/sbin/usermod -G group1,group2,group3,antivir username
```

group1 bis group3 sind dabei die Gruppen, zu denen ein Benutzer schon gehört, username ist der Name des Benutzers.

Um festzustellen, zu welchen Gruppen ein Benutzer gehört:

► Geben Sie ein:

```
/usr/bin/groups
```

**Starten** ► Starten Sie die GUI wie folgt:

```
antivir-gui
```

Falls mit diesem Befehl die Java-Installation nicht gefunden wird:

► Erstellen Sie einen soft-link in /usr/bin (als root):

```
ln -s /PFAD/ZUR/JAVA/INSTALLATION/bin/java /usr/bin
```

**Kommunikation** Die GUI kommuniziert mit AntiVir MailGate mit SSL über das Loopback Netzwerk Interface. Folgende Parameter müssen in der Konfigurationsdatei avmailgate.conf eingetragen sein:

```
GuiSupport      YES
GuiCAFile       /usr/lib/AntiVir/gui/cert/cacert.pem
GuiCertFile     /usr/lib/AntiVir/gui/cert/server.pem
GuiCertPass     antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht die GUI nicht zur Verfügung.

**Mehrere Produkte** Sind mehrere AntiVir-Produkte auf einem Computer installiert, werden diese in der GUI mit je einem Reiter gezeigt. Damit können Sie die einzelnen Produkte leicht überwachen und konfigurieren. Je nachdem, welchen Reiter Sie anklicken, erscheinen die produktspezifischen GUIs und Menüs.

**Probleme** Prüfen Sie bei Problemen mit der GUI, ob folgende Bedingungen erfüllt sind:

- AntiVir MailGate muss in `/usr/lib/AntiVir` installiert sein.
- Es muss eine COMMERCIAL-Lizenz für AntiVir MailGate vorhanden sein (`antivir --version`).
- In der Datei `avmailgate.conf` muss der Parameter für `GuiSupport` gesetzt sein.
- Der Benutzer muss in der "antivir"-Gruppe sein.

Sind diese Bedingungen nicht erfüllt, erscheint die Meldung, dass AntiVir MailGate steht oder dass AntiVir MailGate nicht auf dem Rechner vorhanden ist.

## 6.2 AntiVir MailGate über GUI bedienen

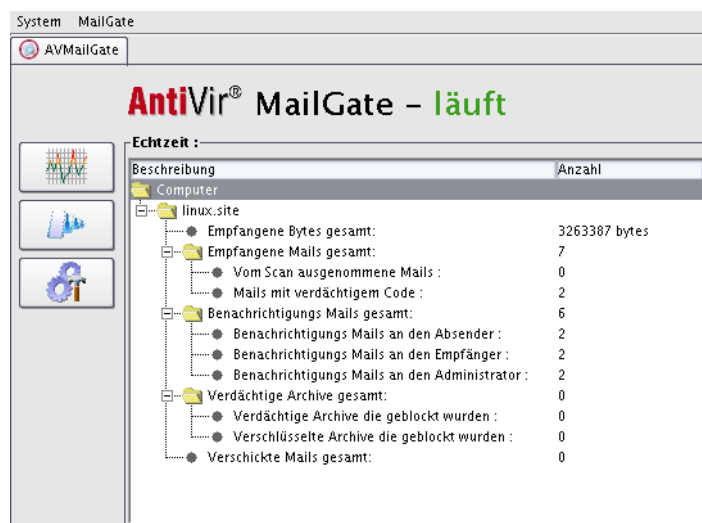
### GUI starten

✓ Damit MailGate mit der GUI kommuniziert, muss der Eintrag `GuiSupport` in `avmailgate.conf` aktiviert sein.

► Starten Sie die GUI:

`/usr/lib/AntiVir/antivir-gui`

↳ Die GUI erscheint mit dem Dialogfenster **Echtzeit**.



Status-  
anzeige

Schrift Mitte oben:

- grüne Schrift (z. B. **läuft**): MailGate ist aktiv
- blaues Fragezeichen: Status von MailGate ist unbekannt
- rote Schrift: MailGate ist nicht aktiv
- gelbe Schrift: MailGate wird neu gestartet

Mehrere  
MailGates

Wurden über das Netzwerk mehrere MailGates ausgewählt, können unterschiedliche Zustände in folgendem Format angezeigt werden (Beispiel):

( 1 | 2 | 1 | 1 )

Erklärung:

- 1 MailGate läuft
- 2 MailGates sind aktiv
- 1 MailGate wird neu gestartet
- von 1 MailGate ist der Status unbekannt

### Symbolleiste



Anklicken schaltet in das Dialogfenster **Echtzeit-Anzeige** um.



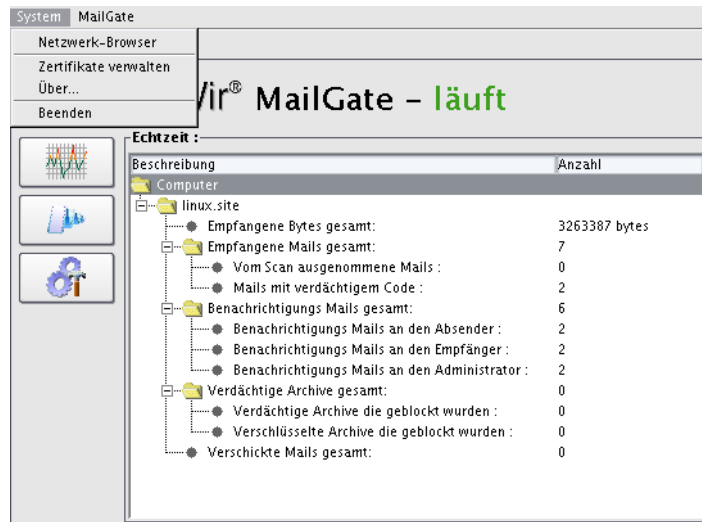
Anklicken schaltet in das Dialogfenster **Logdatei** um.



Anklicken öffnet das Dialogfenster **Konfiguration**.

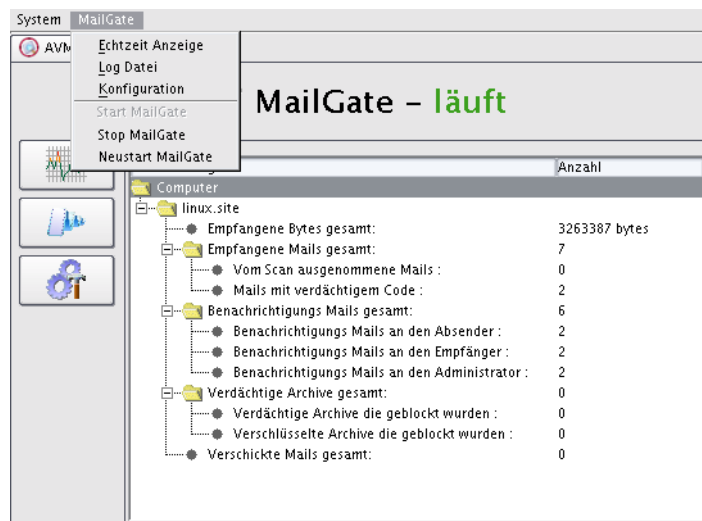
## Menüleiste

### System



- **Netzwerk-Browser:** Zum Auswählen anderer Computer im Netzwerk, auf denen die GUI von MailGate läuft
- **Zertifikate verwalten:** Zum Verwalten bereits integrierter Zertifikate anderer Computer (für künftige Versionen vorgesehen)
- **Über...:** Informationen über die GUI
- **Beenden:** Schließt die GUI. MailGate selbst wird nicht beendet.

### MailGate



- **Echtzeit-Anzeige:** Schaltet in das Dialogfenster **Echtzeit** um
- **Log Datei:** Schaltet in das Dialogfenster **Logdatei** um
- **Konfiguration:** Öffnet das Dialogfenster **Konfiguration**
- **Start MailGate:** Startet MailGate. Der Eintrag ist nur aktiv, wenn MailGate nicht läuft

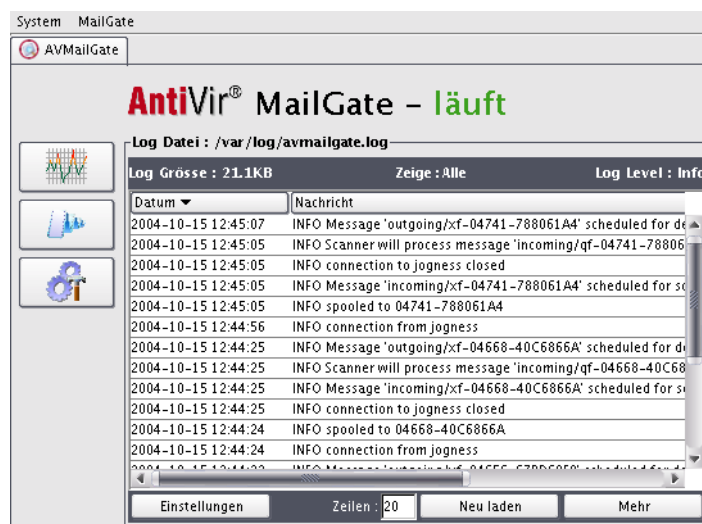
- **Stop MailGate:** Stoppt MailGate. Der Eintrag ist nur aktiv, wenn MailGate läuft
- **Neustart MailGate:** Startet MailGate neu. D. h., MailGate wird beendet und wieder gestartet

### Dialogfenster Echtzeit-Anzeige

Jeder Computer erhält einen eigenen Ordner, in dem verschiedene Email-spezifische Daten festgehalten werden (siehe Abbildung im Abschnitt [GUI starten](#) – Seite 74).

### Dialogfenster Logdatei

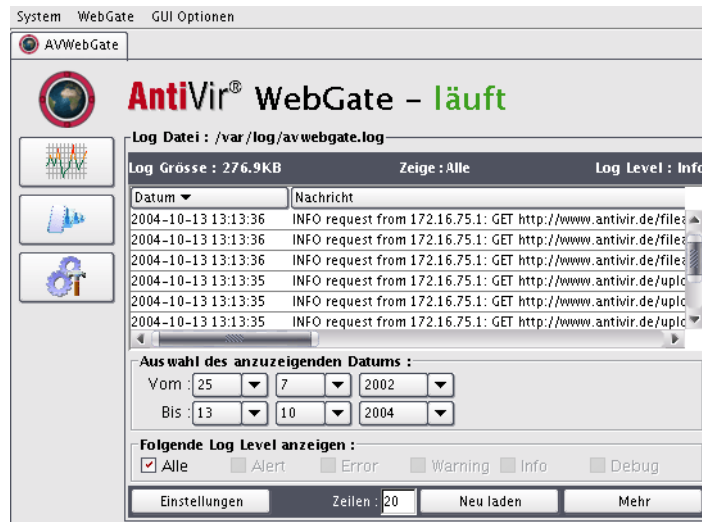
- Klicken Sie auf die mittlere Schaltfläche.  
– ODER –  
Wählen Sie den Menüeintrag **MailGate/Log Datei**.  
↳ Das Dialogfenster **Logdatei** erscheint.



Logdatei Zeigt die komplette Logdatei mit Angabe des Pfads an, darunter die aktuelle Größe der Logdatei in KB, welche Log Level angezeigt werden und welchen Log Level MailGate verwendet.

Unter dem Ausgabefenster befinden sich vier Schaltflächen:  
**Einstellungen, Zeilen, Neu laden und Mehr.**

- Einstellungen
- Klicken Sie auf die Schaltfläche **Einstellungen**.  
↳ Das folgende Dialogfenster erscheint:



- **Auswahl des anzuzeigenden Datums:** Auswahl des Zeitfensters, in dem Einträge der Logdatei angezeigt werden sollen; Standardeinstellung: komplette Logdatei.
- **Folgende Log Level anzeigen:** Auswahl der anzuzeigenden Log Level; Standardeinstellung: **Alle**.

Zeilen    Anzahl der zu ladenden Logzeilen

Neu laden    Logdatei neu laden

Mehr    Bei geladener Logdatei wird die Ansicht um die bei **Zeilen** angegebene Anzahl erweitert.

## Dialogfenster Konfiguration

siehe [AntiVir MailGate über GUI konfigurieren](#) – Seite 79

## MailGate starten und beenden

- Starten    ► Wählen Sie den Menüeintrag **MailGate/Start MailGate**.
- Beenden    ► Wählen Sie den Menüeintrag **MailGate/Stop MailGate**.
- Neu starten    ► Wählen Sie den Menüeintrag **MailGate/Neustart MailGate**.



### GUI beenden

- Wählen Sie den Menüeintrag **System/Beenden**.
  - ↳ Die GUI wird beendet.



Wenn Sie die GUI beenden, bleibt der aktuelle Status von AntiVir MailGate erhalten.

## 6.3 AntiVir MailGate über GUI konfigurieren

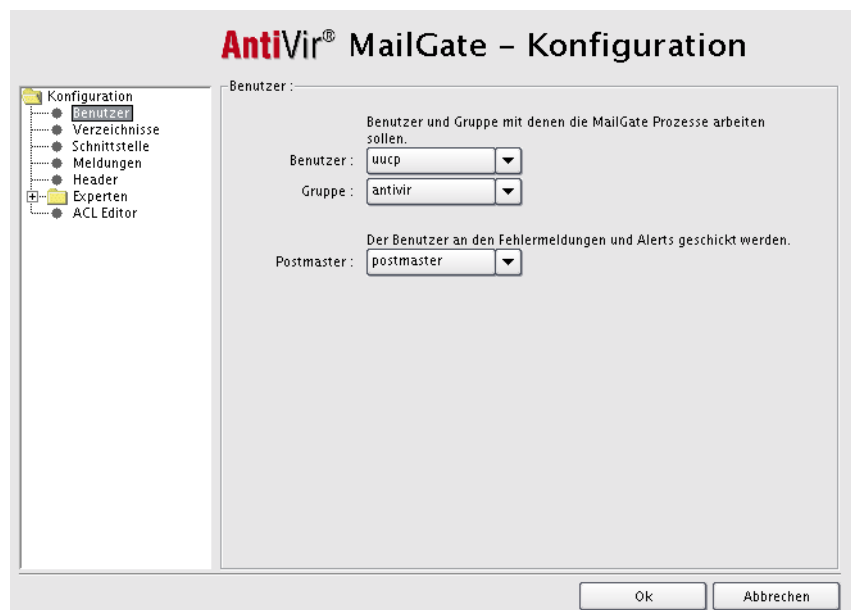
Sie können die Parameter aus der Konfigurationsdatei `avmailgate.conf` über die GUI anpassen.

Zum besseren Verständnis wird für jeden Parameter der entsprechende Eintrag in `avmailgate.conf` aufgeführt. Die Parameter sind im Kapitel [Konfigurieren der Datei avmailgate.conf](#) – Seite 51 ausführlich beschrieben.

### Dialogfenster Konfiguration öffnen



- Klicken Sie auf das Symbol für Konfiguration in der Symbolleiste.
  - ODER –
- Wählen Sie den Menüeintrag **MailGate/Konfiguration**.
  - ↳ Das Dialogfenster **Konfiguration** erscheint:



Bei der Konfiguration wird unterschieden zwischen Einstellungen für "normale" Benutzer und solchen für "Experten".

- ▶ Wählen Sie in der Baumstruktur einen Eintrag.
  - ↳ Ein Dialogfenster mit den Einstellungen für den jeweiligen Bereich erscheint.

### 6.3.1 Einstellungen für "normale" Benutzer

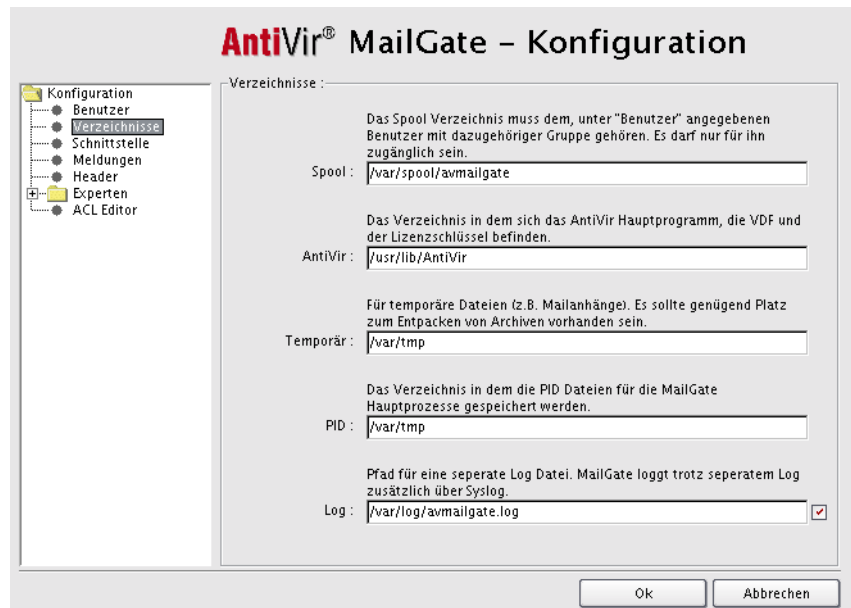
#### Bereich Benutzer

Benutzer    Benutzer und Gruppe, mit denen die MailGate-Prozess arbeiten sollen  
Gruppe    (dies sollte nicht "root" sein). Hierdurch werden `User` und `Group` in `avmailgate.conf` gesetzt.

Wenn diese Einstellungen geändert werden, müssen die Zugriffsrechte auch für die betroffenen Verzeichnisse nachgezogen werden.

Postmaster    Empfänger von Warnungen vor Viren bzw. unerwünschten Programmen sowie anderer Nachrichten. Hierdurch wird `Postmaster` in `avmailgate.conf` gesetzt.

## Bereich Verzeichnisse

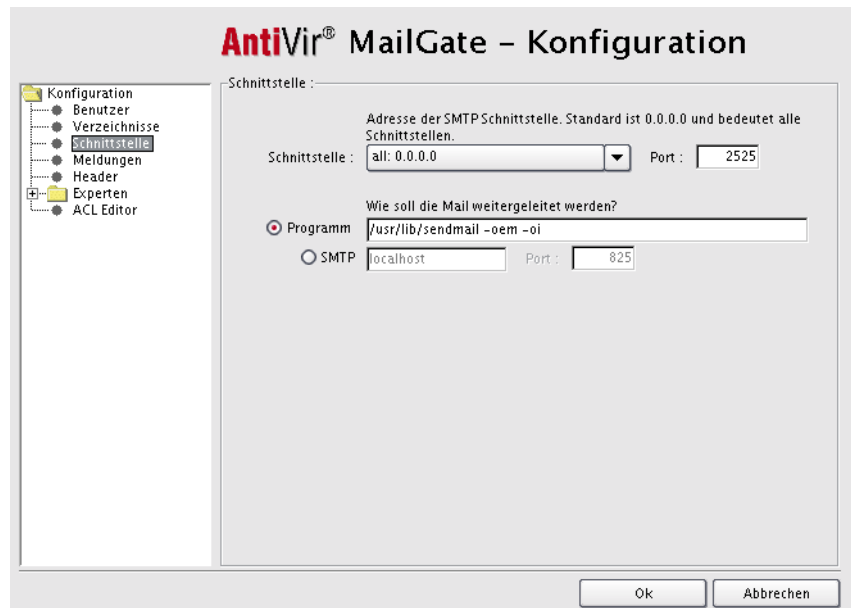


- Spool** In den Unterverzeichnissen incoming, rejected und outgoing werden Emails während des Prozessablaufs abgelegt.
- Das Spool-Verzeichnis muss dem unter Benutzer angegebenen Benutzer mit zugehöriger Gruppe gehören. Es darf nur für ihn zugänglich sein. Hierdurch wird `SpoolDir` in `avmailgate.conf` gesetzt.
- AntiVir** In diesem Verzeichnis befinden sich das AntiVir Hauptprogramm, die Virusdefinitionsdatei `antivir.vdf` und die Lizenzdatei. Hierdurch wird `AntiVirDir` in `avmailgate.conf` gesetzt.
- Temporär** Im temporären Verzeichnis werden die temporären Dateien abgelegt (z. B. Email-Anhänge, die auf Viren bzw. unerwünschte Programme untersucht werden). Für ungepackte Anhänge wird entsprechend ausreichender Platz benötigt. Hierdurch wird `TemporaryDir` in `avmailgate.conf` gesetzt.
- PID** In diesem Verzeichnis werden die PID-Dateien für die MailGate-Hauptprozesse gespeichert (`avgated` und `avgatefwd`). Hierdurch wird `PidDir` in `avmailgate.conf` gesetzt.
- Log** Die Angabe muss den vollständigen Pfad zu einer separaten Logdatei enthalten. Wenn das Kontrollkästchen nicht aktiviert ist, wird keine separate Logdatei verwendet. Hierdurch wird `LogFile` in `avmailgate.conf` gesetzt.



Unabhängig davon, ob eine separate Logdatei aktiv ist, werden grundsätzlich Einträge an den syslog gesendet.

### Bereich Schnittstelle



**Schnittstelle** Schnittstelle und Port, an denen der SMTP-Dämon lauscht. AntiVir MailGate lauscht standardmäßig an allen Netzwerkkarten (bei 0.0.0.0). Sie können jedoch auch eine IP-Adresse für eine einzelne Netzwerkkarte angeben. Wenn Sie unsicher sind, lassen Sie die Standardeinstellung unverändert.

Hierdurch wird `ListenAddress` in `avmailgate.conf` gesetzt.

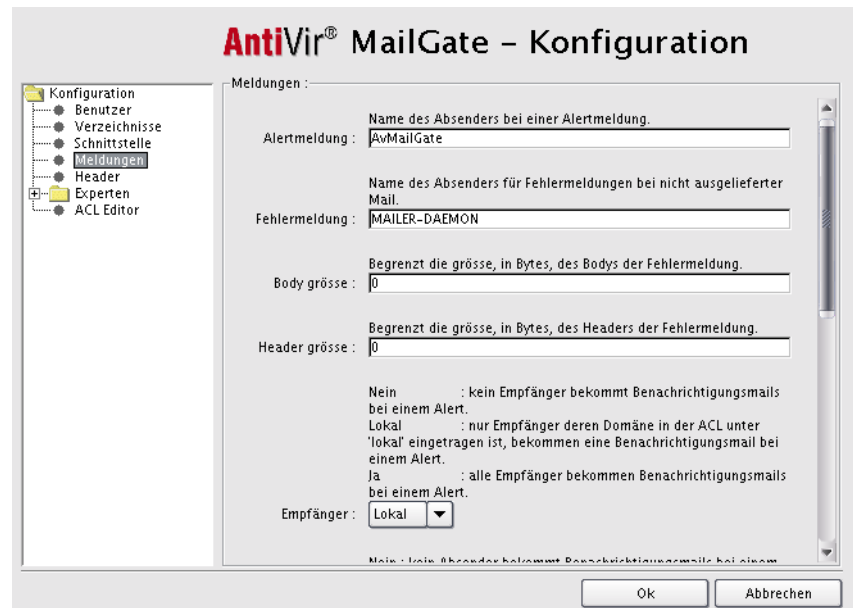
**Programm** Definiert, wie die Email weitergeleitet werden soll, Standardeinstellung ist das Versenden per sendmail.

**SMTP**

Die Email kann jedoch auch per SMTP weitergeleitet werden.

Hierdurch wird `ForwardTo` in `avmailgate.conf` gesetzt.

## Bereich Meldungen



- |               |  |
|---------------|--|
| Alertmeldung  | Benutzername oder Email-Adresse des Absenders von Warnungen (wenn ein Virus bzw. unerwünschtes Programm in einer Email gefunden wurde). Hierdurch wird <code>AlertsUser</code> in <code>avmailgate.conf</code> gesetzt.  |
| Fehlermeldung | Der Absender von Fehlermeldungen, wenn eine Email nicht ausgeliefert werden konnte, ist der hier angegebene Name. Hierdurch wird <code>BounceMessageUser</code> in <code>avmailgate.conf</code> gesetzt.   |
| Body Größe    | Begrenzt die Größe des Bodys der Bouncemail (in Bytes). Die Angabe 0 bedeutet kein Limit. Hierdurch wird <code>BounceMessageSizeBody</code> in <code>avmailgate.conf</code> gesetzt.   |
| Header Größe  | Begrenzt die Größe des Headers der Bouncemail (in Bytes). Die Angabe 0 bedeutet kein Limit. Hierdurch wird <code>BounceMessageSizeHeader</code> in <code>avmailgate.conf</code> gesetzt.   |
| Empfänger     | <p>Es können Warnungen vor Viren bzw. unerwünschten Programmen an die Empfänger gesendet werden. Folgende Möglichkeiten gibt es:</p> <ul style="list-style-type: none"> <li>● <b>Nein:</b> Es werden keine Warnungen an die Empfänger gesendet.</li> <li>● <b>Lokal:</b> Warnungen werden nur gesendet, wenn der Empfänger ein lokaler Benutzer Ihrer Domäne ist. Dies legen Sie in der Datei <code>avmailgate.acl</code> mit der Option <code>local</code> fest.</li> <li>● <b>Ja:</b> Es werden immer Warnungen an die Empfänger gesendet.</li> </ul> <p>Hierdurch wird <code>ExposeRecipientsAlerts</code> in <code>avmailgate.conf</code> gesetzt.</p> |
| Absender      | Es können Warnungen vor Viren bzw. unerwünschten Programmen an den Absender gesendet werden. Folgende Möglichkeiten gibt es:   |

- **Nein:** Es wird keine Warnung an den Absender der betroffenen Email gesendet.
- **Local:** Eine Warnung wird nur gesendet, wenn der Absender ein lokaler Benutzer Ihrer Domäne ist. Dies legen Sie in der Datei `avmailgate.acl` mit der Option `local` fest.
- **Ja:** Es wird immer eine Warnung an den Absender der betroffenen Email gesendet.

Hierdurch wird `ExposeSenderAlerts` in `avmailgate.conf` gesetzt.

**Postmaster** Sendet Warnungen vor Viren bzw. unerwünschten Programmen an den Postmaster. Mögliche Einstellungen sind **Ja** oder **Nein**.  
Hierdurch wird `ExposePostmasterAlerts` in `avmailgate.conf` gesetzt.

**Mail Header** Sie können den Header der verdächtigen Email in die Benachrichtigungs-Email an den Postmaster einfügen. Mögliche Einstellungen sind **Ja** oder **Nein**.  
Hierdurch wird `AddHeaderToNotice` in `avmailgate.conf` gesetzt.

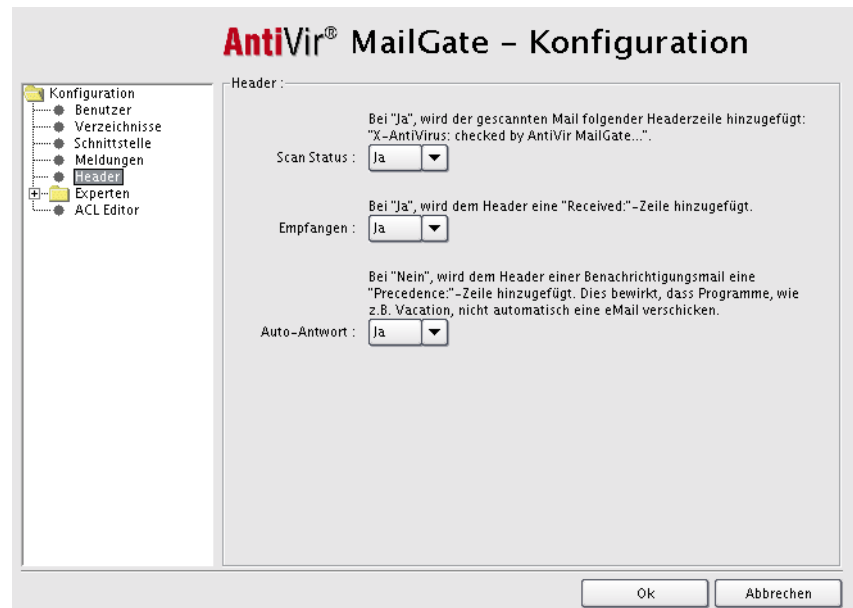
**Status** Wenn **NO** eingestellt ist, wird in die weitergeleitete Email keine Nachricht eingefügt.  
Wenn **YES** eingestellt ist:

- Einfache RFC822-Email (keine MIME-Email): Nachricht wird an den Anfang der Email eingefügt.
- MIME-Email: Geprüfte Email als eine neue MIME multipart/mixed Email weiterleiten, mit einem Textabschnitt, der die Mitteilung über den Status beinhaltet, und einem zweiten RFC822-Abschnitt, der die gesamte Original-Email enthält. Die meisten Header vom Original werden in die weitergeleitete Nachricht kopiert.
- Wenn im Template-Verzeichnis eine Datei `body-state` existiert, wird der darin enthaltene benutzerdefinierte Text in die Email eingefügt (siehe [Konfigurieren der Vorlagen für Nachrichten](#) – Seite 66).

Hierdurch wird `AddStatusInBody` in `avmailgate.conf` gesetzt.

**Lizenz** Sendet eine Meldung an den postmaster, wann die Lizenz von AntiVir abläuft (Angabe in Tagen). Die Angabe 0 bedeutet keine Meldung.  
Hierdurch wird `NotifyEndOfLicense` in `avmailgate.conf` gesetzt.

## Bereich Header



**Scan Status** Wenn **Ja** eingegeben ist, wird der gescannten Email folgende Headerzeile hinzugefügt: X-AntiVirus: checked by AntiVir MailGate... Der Text ist nicht modifizierbar.

Hierdurch wird AddXHeader in avmailgate.conf gesetzt.

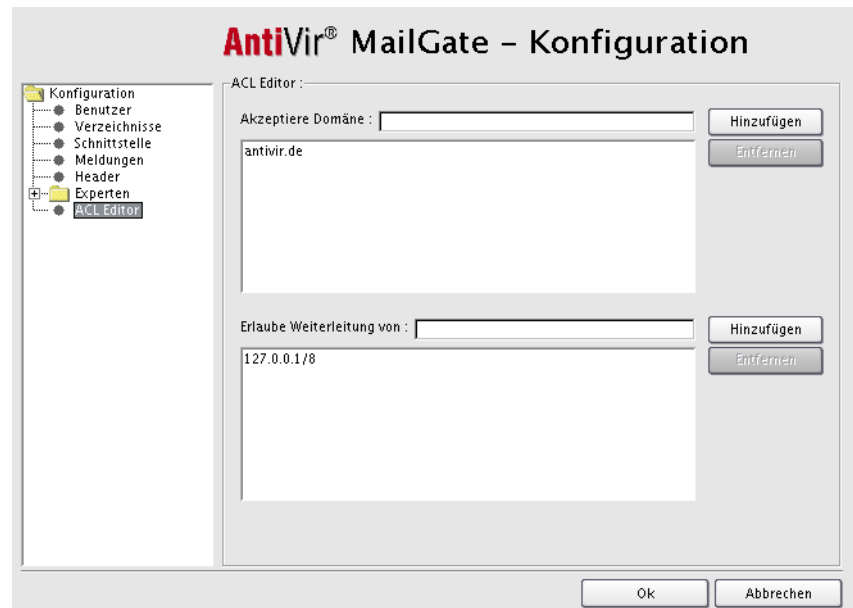
**Empfangen** Wenn **Ja** eingegeben ist, erhält die gescannte Email einen Vermerk im Header, wann sie eingegangen ist.

Hierdurch wird AddReceivedByHeader in avmailgate.conf gesetzt.

**Auto-Antwort** Diese Option ist nur in der Professional Edition verfügbar. Wenn **Ja** eingestellt ist, erhält die beim Fund eines Virus bzw. unerwünschten Programms versandte Email den Vermerk **Precedence: junk**. Programme, die auf eingegangene Emails automatisch antworten (z. B.: vacation), reagieren dann nicht auf diese Benachrichtigungs-Email.

Hierdurch wird AddPrecedenceHeader in avmailgate.conf gesetzt.

### ACL Editor



In der Datei avmailgate.acl wird anhand der Schlüsselwörter local und relay festgelegt, welchen Rechnern das Verschicken von Emails über AntiVir MailGate erlaubt wird. Dies wird über die Absender- und/oder Empfänger-Domäne bzw. die IP-Adresse festgelegt.

Akzeptiere Domäne ► Legen Sie fest, welche Hosts und/oder Domänen lokal sind, z. B. localhost oder antivir.de.

Erlaube Weiterleitung von ► Legen Sie fest, welche Hosts und Netzwerke Emails verschicken dürfen, z. B. 127.0.0.1/8 oder 192.168.0.0/16.

#### IP-Adressen:

Sie können IP-Adressen auf verschiedene Art und Weise angeben:

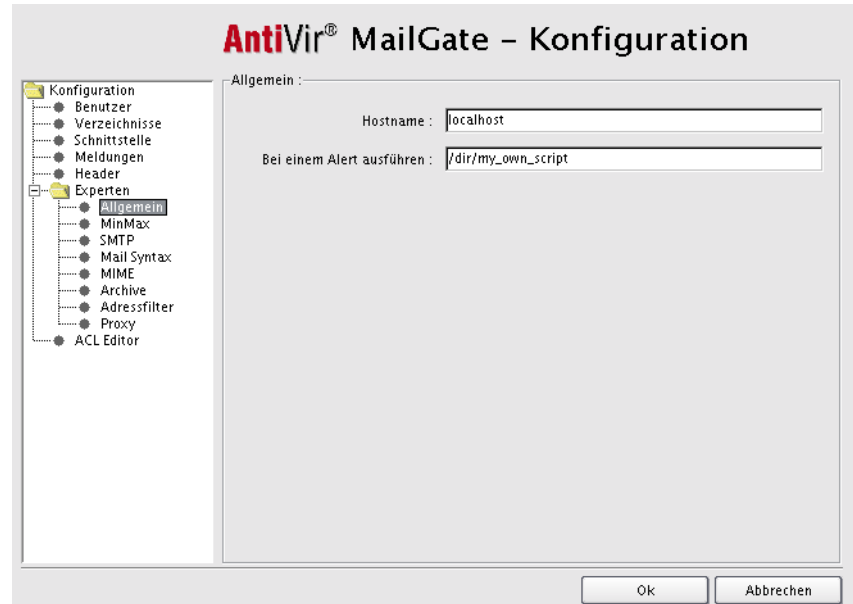
192.168.0.0/16 oder 192.168

haben die gleiche Bedeutung. /16 bedeutet 16 bit und bezeichnet die ersten beiden Zahlen der IP-Adresse. D. h., es sind alle IP-Adressen erlaubt, die mit 192.168 beginnen.



## 6.3.2 Einstellungen für Experten

### Bereich Allgemein



Hostname FQDN (Fully Qualified Domain Name) des lokalen Hosts.

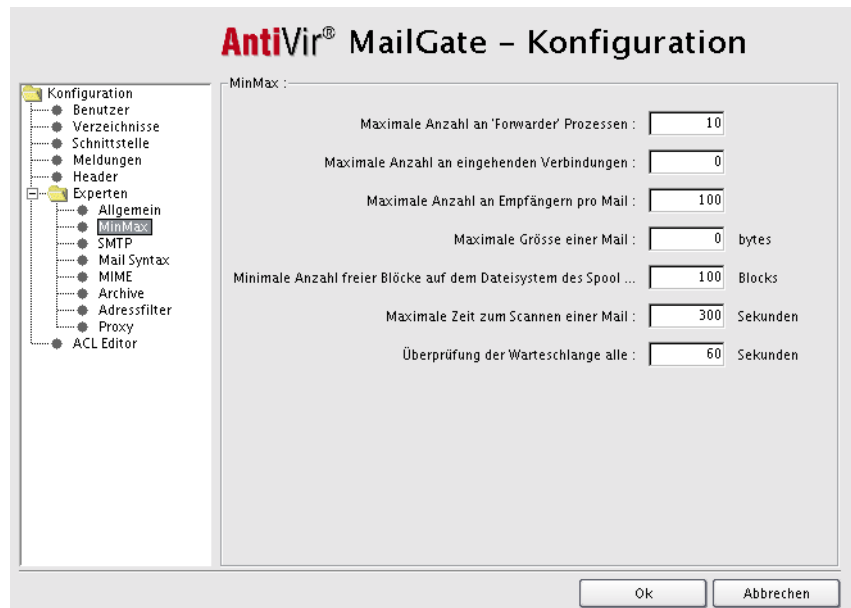
Wenn dieses Eingabefeld leer ist, ist die Standardeinstellung der hostname, der von `gethostname(2)` zurückgegeben wird. Andernfalls ist localhost voreingestellt:

Hierdurch wird `MyHostName` in `avmailgate.conf` gesetzt.

Bei einem Alert ausführen Ruft ein externes Programm oder ein Skript auf, wenn ein Virus bzw. unerwünschtes Programm gefunden wurde. Der Parameter ist die ID der zurückgewiesenen Email (siehe [Arbeitsweise von AntiVir MailGate beim Fund von Viren oder unerwünschten Programmen](#) – Seite 50).

Hierdurch wird `ExternalProgram` in `avmailgate.conf` gesetzt.

### Bereich MinMax



Max. Anzahl  
an Forwarder  
Prozessen

Maximale Anzahl der Weiterleitungsprozesse (avgatefwd), die gleichzeitig laufen können. Der Wert ist abhängig von der Leistungsfähigkeit Ihres Email-Systems und der Qualität Ihrer Netzwerkverbindung (Standardeinstellung: 10).

Hierdurch wird `MaxForwarders` in `avmailgate.conf` gesetzt.

Max. Anzahl  
gleichzeitig  
eingehender  
Verbindungen

Begrenzt die Anzahl gleichzeitiger Verbindungen von der Remote-Site. Sie können z. B. angeben, dass maximal 100 Emails gleichzeitig eingehen können. Der Wert 0 (Standardeinstellung) schaltet diese Option aus; d. h. es können unbegrenzt viele Emails passieren.

Hierdurch wird `MaxIncomingConnections` in `avmailgate.conf` gesetzt.

Max. Anzahl  
an Empfängern pro  
Email

Definiert die maximale Anzahl der Empfänger, die eine Nachricht erhalten können. Der Wert 0 schaltet diese Option aus.

Hierdurch wird `MaxRecipientsPerMessage` in `avmailgate.conf` gesetzt.

Max. Größe  
einer Email

Wenn ein Wert >0 Bytes eingestellt ist, werden nur Emails bis zu dieser Größe überprüft. Größere Emails werden abgewiesen.

Wenn der Wert 0 eingestellt ist, werden Emails unabhängig von ihrer Größe überprüft.

Hierdurch wird `MaxMessageSize` in `avmailgate.conf` gesetzt.

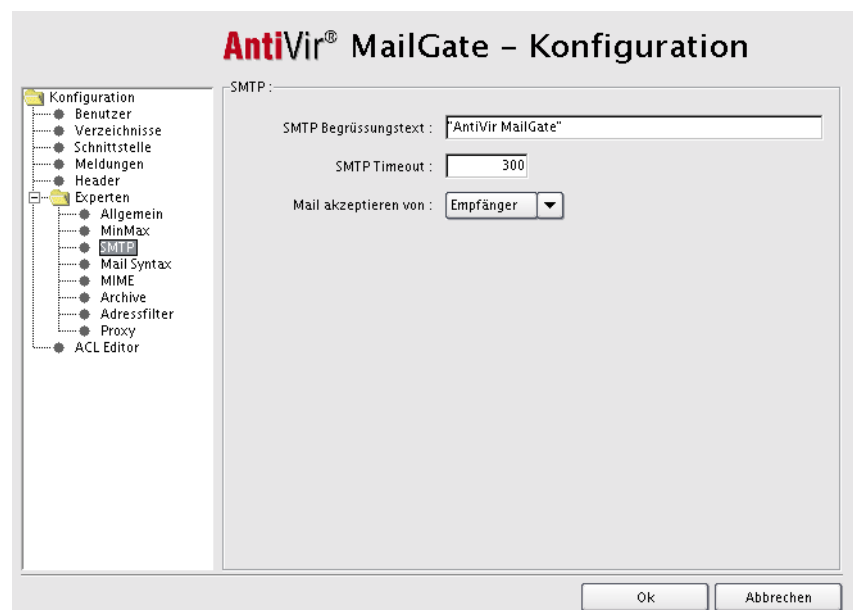
Freie Blöcke  
auf dem  
Dateisystem  
des Spool-  
Verzeichnisses

AntiVir MailGate blockt eingehende Verbindungen ab, wenn die Anzahl der freien Blöcke im Dateisystem (also der Speicherplatz auf der Festplatte) kleiner als der angegebene Wert ist.

Hierdurch wird `MinFreeBlocks` in `avmailgate.conf` gesetzt.

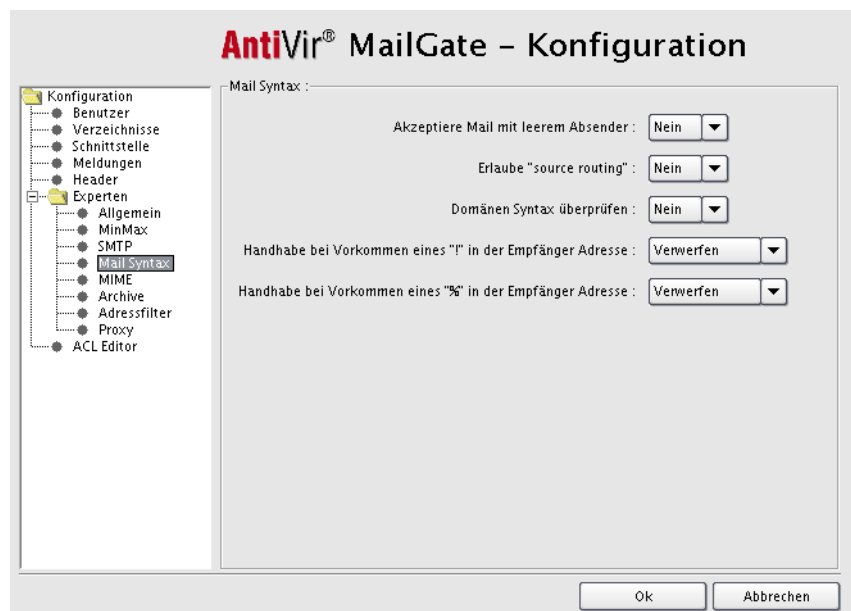
- |                                   |  |
|-----------------------------------|--|
| Max. Zeit zum Scannen einer Email | Definiert die maximale Dauer des Email-Scans in Sekunden. Hierdurch wird <code>ScanTimeOut</code> in <code>avmailgate.conf</code> gesetzt.   |
| Überprüfung der Warteschlange     | Legt das Zeitintervall in Sekunden fest, wann <code>avgatefd</code> die Warteschlange nach neuen Emails durchsuchen soll, um sie auf Viren bzw. unerwünschte Programme zu prüfen.<br><br>Hierdurch wird <code>PollPeriod</code> in <code>avmailgate.conf</code> gesetzt. |

### Bereich SMTP



- |                       |  |
|-----------------------|--|
| SMTP Begrüssungstext  | Meldungszeile, die MailGate an den Mailserver ausgibt. Sie können den Text editieren, z. B. wenn die Art der eingesetzten Virenschutz-Software nicht bekannt gegeben werden soll.<br><br>Hierdurch wird <code>SMTPBanner</code> in <code>avmailgate.conf</code> gesetzt.   |
| SMTP Timeout          | Definiert die maximale Dauer der SMTP-Connection in Sekunden. Hierdurch wird <code>SMTPTimeout</code> in <code>avmailgate.conf</code> gesetzt.   |
| Email akzeptieren von | Mit dieser Option wird festgelegt, ob die Domänen-Namen der Empfängeradressen (RECIPIENT), der Absenderadressen (SENDER) oder beider Adressen (BOTH) auf die Einträge in dem <code>local:-</code> Abschnitt in der Datei <code>avmailgate.acl</code> geprüft werden sollen.<br><br>Hierdurch wird <code>MatchMailAddressForLocal</code> in <code>avmailgate.conf</code> gesetzt.<br><br>Nähere Informationen finden Sie im Kapitel <a href="#">Konfigurieren der Datei <code>avmailgate.acl</code></a> – Seite 64. |

### Bereich Mail Syntax



Akzeptiere  
Email mit  
leerem  
Absender

Es ist möglich, Emails mit leerem Absender abzulehnen. Die Standardeinstellung ist **Nein**, d. h. der SMTP-Server akzeptiert alle eingehenden Emails. Diese Einstellung sollte nicht geändert werden.

Hierdurch wird `RefuseEmptyMailFrom` in `avmailgate.conf` gesetzt.



RFC2821, RFC821 und RFC2505 empfehlen, dass ein SMTP-Server alle Emails (auch ohne Absenderadresse) annehmen muss. Es wird empfohlen, die Standardeinstellung des Parameters `RefuseEmptyMailFrom` nicht zu ändern.

Erlaube  
"source  
routing"

Source routing wird durch folgende Adress-Syntax erreicht:

```
@ONE, @TWO:JOE@THREE
```

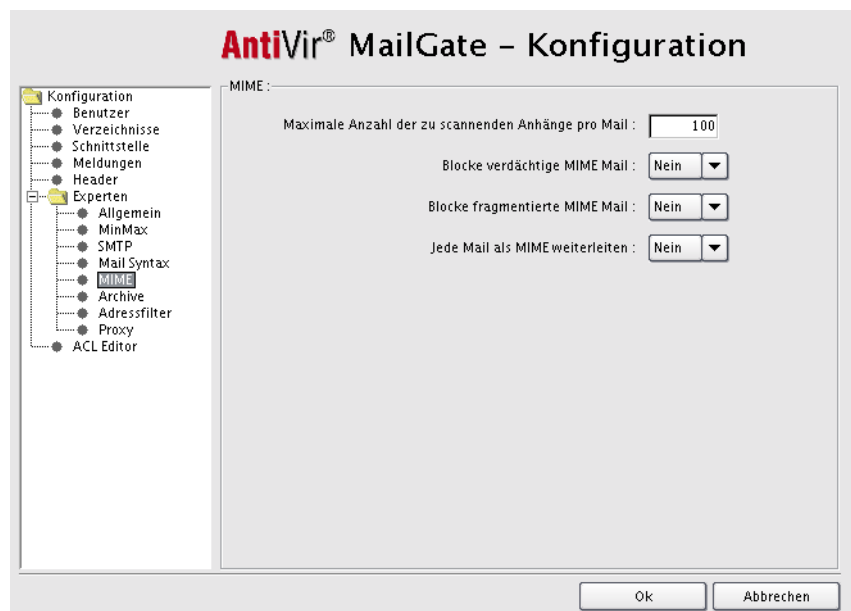
Damit wird definiert, welchen Weg eine Email nehmen soll: Sie soll über ONE und TWO und schliesslich an JOE auf dem Host THREE ausgeliefert werden.

Mit dieser Option legen Sie fest, ob alles außer `JOE@THREE` entfernt (**Nein**) oder ob die Adresse beibehalten werden soll (**Ja**).

Hierdurch wird `AllowSourceRouting` in `avmailgate.conf` gesetzt.

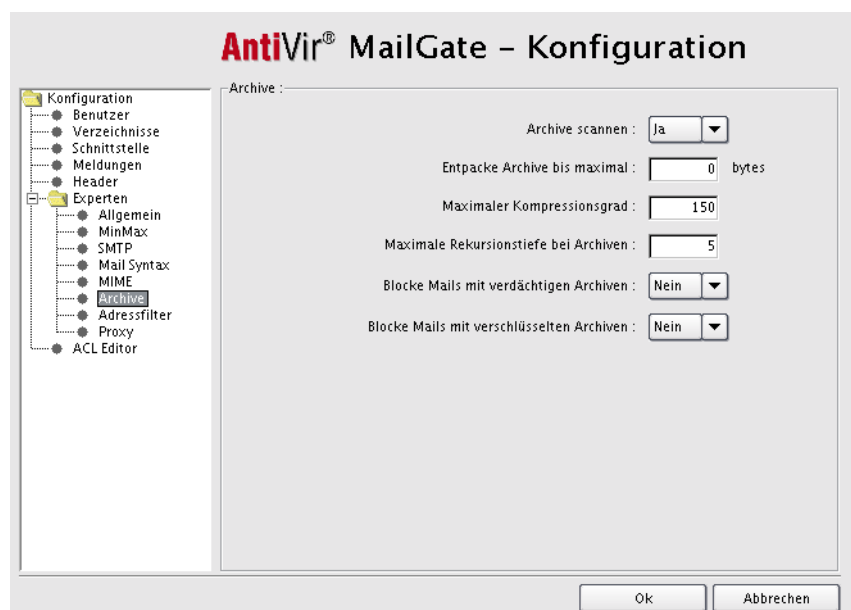
Domänen-Syntax überprüfen	<p>Ein Domänen-Name darf nur aus folgenden Zeichen bestehen: [-.0-9A-Za-z]. Es ist jedoch auch möglich, nicht korrekte Domänen-Namen zuzulassen.</p> <p>Wenn <b>Nein</b> eingestellt und der Domänen-Name für die Zustellung der Meldung nicht korrekt ist (abhängig vom Source-Routing), wird die Meldung zurückgewiesen.</p> <p>Wenn <b>Ja</b> eingestellt ist, wird der Domänen-Name nicht geprüft; d. h., auch Emails mit nicht korrektem Domänen-Namen werden weitergeleitet.</p> <p>Hierdurch wird <code>AcceptLooseDomainName</code> in <code>avmailgate.conf</code> gesetzt.</p>
"!" in der Empfängeradresse	<p>Wenn <b>Verwerfen</b> eingestellt und ein "!" in der Empfängeradresse ist, wird die Meldung zurückgewiesen.</p> <p>Wenn <b>Ignorieren</b> eingestellt ist, wird ein "!" wie ein normales Zeichen der Empfängeradresse behandelt.</p> <p>Wenn <b>Interpretieren</b> eingestellt ist, wird die Empfängeradresse in eine RFC821-gemäße Standardform umgewandelt. Z. B. wird die Adresse</p> <pre>hostA!hostB!hostC!user</pre> <p>umgewandelt in</p> <pre>hostA,@hostB:user@hostC</pre> <p>Wenn Source-Routing erlaubt ist, wird die Email an hostA gesendet, andernfalls an hostC.</p> <p>Hierdurch wird <code>InEnvelopeAddressesBangIs</code> in <code>avmailgate.conf</code> gesetzt.</p>
"%" in der Empfängeradresse	<p>Wenn <b>Verwerfen</b> eingestellt und ein "%" in der Empfängeradresse ist, wird die Meldung zurückgewiesen.</p> <p>Wenn <b>Ignorieren</b> eingestellt ist, wird ein "%" wie ein normales Zeichen der Empfängeradresse behandelt.</p> <p>Wenn <b>Interpretieren</b> eingestellt ist, wird die Empfängeradresse in eine RFC821-gemäße Standardform umgewandelt. Z. B. wird die Adresse</p> <pre>user%hostC%hostB@hostA</pre> <p>umgewandelt in</p> <pre>@hostA,@hostB:user@hostC</pre> <p>Wenn Source-Routing erlaubt ist, wird die Email an hostA gesendet, andernfalls an hostC.</p> <pre>InEnvelopeAddressesPercentIs    REFUSED</pre> <p>Hierdurch wird <code>InEnvelopeAddressesPercentIs</code> in <code>avmailgate.conf</code> gesetzt.</p>

### Bereich MIME



- |                                   |   |
|-----------------------------------|---|
| Anhänge pro Email                 | Definiert die maximale Anzahl der zu scannenden Anhänge pro MIME-Email.<br>Hierdurch wird <code>MaxAttachments</code> in <code>avmailgate.conf</code> gesetzt.  |
| Blocke verdächtige MIME-E-mails   | Blockt die Weiterleitung verdächtiger MIME-E-mails. Eine MIME-Email wird als verdächtig eingestuft, wenn die maximale Zahl von Anhängen erreicht ist.<br>Hierdurch wird <code>BlockSuspiciouMime</code> in <code>avmailgate.conf</code> gesetzt.  |
| Blocke fragmentierte MIME-E-mails | Blockt Emails, die beschädigt zugestellt werden. Weitere Informationen siehe "Message Fragmentation and Reassembly", RFC 2046, <a href="http://www.faqs.org/rfcs/rfc2046.html">http://www.faqs.org/rfcs/rfc2046.html</a> , Abschnitt 5.2.2.1).<br>Hierdurch wird <code>BlockFragmentedMessage</code> in <code>avmailgate.conf</code> gesetzt.   |
| Jede Email als MIME weiterleiten  | Emails, die nicht als MIME-E-mails ankommen, können zu MIME-E-mails umgeschrieben werden. Sie bekommen einen MIME-Header, mit Content-Type: text/plain, Content-Disposition: inline und einem Content-Encoding: 7 bit oder 8 bit. Das "Encoding" hängt von der ursprünglichen Email ab.<br>Hierdurch wird <code>ForwardAllEmailAsMIME</code> in <code>avmailgate.conf</code> gesetzt. |

## Bereich Archive



Archive  
scannen

Wenn **Nein** eingestellt ist, werden Archive nicht auf Viren bzw. unerwünschte Programme durchsucht.

Wenn **Ja** eingestellt ist, werden alle Dateien in Archiven dekomprimiert und durchsucht – abhängig von den drei folgenden Einstellungen.

Hierdurch wird `ScanInArchive` in `avmailgate.conf` gesetzt.

Entpacke  
Archive  
bis max.



Es gibt komprimierte Dateien, die keinen sinnvollen Inhalt haben, aber bewusst so angelegt sind, dass sie sich auf "unsinnige Größe" aufblähen, um den Rechner lahm zu legen. Dieser Parameter schützt vor dem Entpacken solcher Archiv-Dateien.

Wenn der Wert 0 Bytes eingestellt ist, werden alle Dateien in Archiven entpackt – unabhängig von ihrer Größe.

Wenn ein Wert >0 Bytes eingestellt ist, werden nur die Dateien durchsucht, die im entpackten Zustand nicht größer als dieser Wert sind.

Hierdurch wird `ArchiveMaxSize` in `avmailgate.conf` gesetzt.

Max.  
Kompressi-  
onsgrad

Blockt so genannte "Mailbomben" mit einer sehr hohen Kompressionsdichte.

Der Wert 0 schaltet diese Option aus. Diese Einstellung wird **nicht** empfohlen.

Hierdurch wird `ArchiveMaxRatio` in `avmailgate.conf` gesetzt.

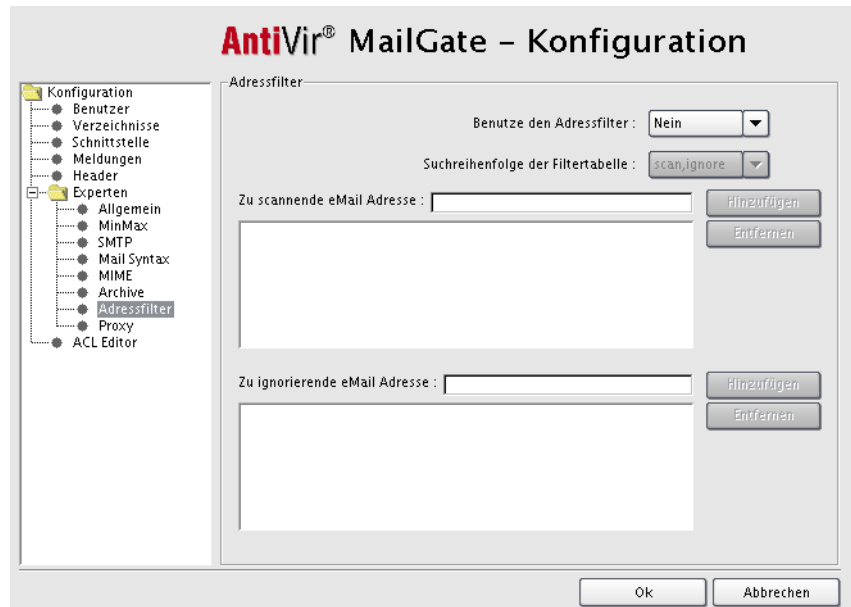
- Max. Rekursionstiefe      Wenn der Wert 0 eingestellt ist, werden rekursive (verschachtelte) Archive vollständig entpackt – unabhängig von der Rekursionstiefe.
- Wenn ein Wert >0 eingestellt ist, werden Archive nur bis zu der angegebenen Rekursionstiefe entpackt. Hierdurch lässt sich Zeit sparen.
- Hierdurch wird `ArchiveMaxRecursion` in `avmailgate.conf` gesetzt.
- Blocke Emails mit verdächtigen Archiven      Wenn **Ja** eingestellt ist, können Emails mit verdächtigen Archiven abgewiesen werden – abhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`.
- Wenn **Nein** eingestellt ist, werden Emails unabhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio` zugestellt.
- Hierdurch wird `BlockSuspiciousArchive` in `avmailgate.conf` gesetzt.
- Blocke Emails mit verschlüsselten Archiven      Wenn **Ja** eingestellt ist, werden Emails abgewiesen, wenn sie Passwort-geschützte Dateien in einem Archiv enthalten.
- Wenn **Nein** eingestellt ist, werden Emails auch zugestellt, wenn sie Passwort-geschützte Dateien in einem Archiv enthalten.
- Hierdurch wird `BlockEncryptedArchive` in `avmailgate.conf` gesetzt.



## Bereich Adressfilter

Die Einstellungen in diesem Bereich betreffen die Dateien avmailgate.scan und avmailgate.ignore. Diese liegen im Verzeichnis /etc.

Nähere Informationen zu diesem Thema finden Sie unter [AddressFilter](#) – Seite 56.



Benutze den Adressfilter

► Wählen Sie **Ja** oder **Nein**.

Nähere Informationen finden Sie unter [AddressFilter](#) – Seite 56.

Suchreihenfolge der Filtertabelle

### Suchreihenfolge der Filtertabelle:

Die Option ist nur bei aktiviertem Adressfilter (Adressfilter **Ja**) von Bedeutung. Mögliche Parameter sind:

```
scan,ignore
- ODER -
ignore,scan
```

Hierdurch wird BlockEncryptedArchive in avmailgate.conf gesetzt.

Zu scannende Email-Adresse

► Tragen Sie hier die entsprechenden Email-Adressen ein.

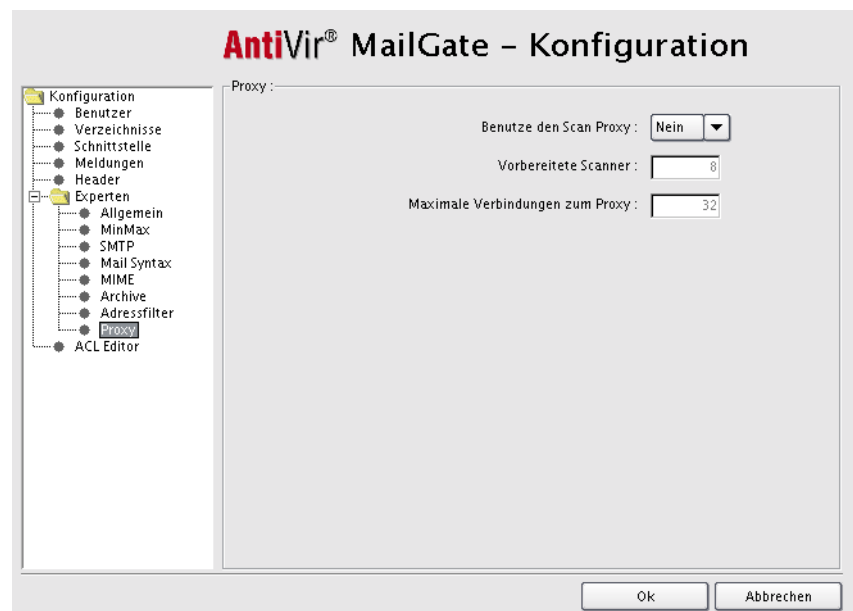
↳ Die Email-Adressen werden in der Datei avmailgate.scan gespeichert.

Zu ignorierende Email-Adresse

► Tragen Sie hier die entsprechenden Email-Adressen ein.

↳ Die Email-Adressen werden in der Datei avmailgate.ignore gespeichert.

### Bereich Proxy



Benutze den  
Scan Proxy

Scans werden mit der Proxy-Option in SAVAPI effektiver ausgeführt, wenn sie einen festgelegten Pool an AntiVir-Scannern verwenden. Da dieser Pool den Durchsatz erhöht, muss die Größe des Pools sehr genau bestimmt werden: Zu viele Scanner verbrauchen zu viel Ressourcen, ohne die Leistung zu steigern, zu wenige Scanner führen dazu, dass die SAVAPI-Anwendungen unnötig lange warten. Mögliche Einstellungen sind YES oder NO.

Hierdurch wird `UseProxy` in `avmailgate.conf` gesetzt.

Vorbereitete  
Scanner

Anzahl der AntiVir-Scanner im Pool (siehe auch `UseProxy`).

Hierdurch wird `ProxyScanners` in `avmailgate.conf` gesetzt.

Max. Verbin-  
dungen zum  
Proxy

Anzahl der maximal zulässigen, gleichzeitigen Verbindungen zwischen AntiVir MailGate und Scanner-Pool.

Hierdurch wird `ProxyConnections` in `avmailgate.conf` gesetzt.

## 7 Service

### 7.1 Support

- Support-Service** Auf unserer Webseite <http://www.antivir.de> erhalten Sie alle Informationen zu unserem umfangreichen Support-Service.
- Die Kompetenz und Erfahrung unserer Entwickler stehen Ihnen hier zur Verfügung. Die Experten der H+BEDV Datentechnik GmbH beantworten Ihre Fragen und helfen bei kniffligen technischen Problemen weiter.
- Während der ersten 30 Tage nach Erwerb einer Lizenz haben Sie die Möglichkeit, den **AntiVir Installationssupport** in Anspruch zu nehmen, telefonisch, per Email oder per Online-Formular.
- Darüber hinaus empfehlen wir Ihnen optional den Erwerb unseres **AntiVir Classic Supports**, mit dem Sie bei auftretenden technischen Problemen unsere Fachleute während der Geschäftszeiten kontaktieren und zu Rate ziehen können. Pro Jahr berechnen wir Ihnen für diesen Service, in dem auch der Virenbereinigungs- und Hoax-Support eingeschlossen sind, zwanzig Prozent des Listenpreises Ihres jeweils erworbenen AntiVir-Programms.
- Der ebenfalls optional verfügbare **AntiVir Premium Support** bietet Ihnen über den Leistungsumfang des AntiVir Classic Supports hinaus genügend Spielraum, auch bei Notfällen außerhalb der Geschäftszeiten jederzeit einen kompetenten Ansprechpartner zu erreichen. Bei Virenalarm wird auf Wunsch eine SMS-Benachrichtigung auf Ihr Mobiltelefon gesendet.
- Forum** Bevor Sie die Hotline kontaktieren, empfehlen wir einen Besuch in unserem Benutzerforum unter <http://forum.antivir.de>. Möglicherweise sind hier schon Ihre Fragen von anderen Benutzern gestellt und beantwortet worden.
- Email-Support** Support über Email erhalten Sie über <http://www.antivir.de>.

### 7.2 Online-Shop

Sie wollen unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der H+BEDV Datentechnik GmbH können Sie unter <http://www.antivir.de> schnell und sicher Lizenzen erwerben, verlängern oder erweitern. Der Online-Shop führt Sie Schritt für Schritt durch das Bestell-Menü. Ein multilinguales Customer-Care-Center informiert Sie über Bestellprozesse, Zahlungsabwicklungen und Auslieferung. Wiederverkäufer können auf Rechnung bestellen und ein Reseller-Panel nutzen.

### 7.3 Kontakt

Postadresse    H+BEDV Datentechnik GmbH  
                    Lindauer Strasse 21  
                    D-88069 Tettnang  
                    Deutschland

Internet        Allgemeine Informationen zu uns und unseren Produkten erhalten Sie  
                    auf unserer Homepage <http://www.antivir.de>.

## 8 Anhang

### 8.1 Glossar

<b>Begriff</b>	<b>Erklärung</b>
Cron-Dämon	Dämon, der andere Programme zu vorgegebenen Zeiten startet
Dämon	Im Hintergrund laufender Prozess zur Systemverwaltung unter UNIX. Im Schnitt laufen einige Dutzend Dämonen auf dem Rechner. Diese Prozesse werden beim Hochfahren des Rechners gestartet.
Demoversion	Ohne Lizenzdatei läuft AntiVir MailGate als Demoversion. Dabei wird in jede Email ein Werbebanner von H+BEDV eingefügt. Ein automatisches Update ist nicht möglich, d. h. neue Virendefinitions-Dateien und eine neue Scan Engine müssen immer manuell von der Webseite heruntergeladen werden.
Eicar	European Institute for Computer Antivirus Research, bietet u. a. die Möglichkeit, mit einem Testvirus Antiviren-Programme zu prüfen. Nähere Informationen unter <a href="http://www.eicar.org">http://www.eicar.org</a>
GPL	General Public License: alternatives Vertriebskonzept, das im weitesten Sinne mit "Shareware" vergleichbar ist
Logdatei	auch: Reportdatei, Protokolldatei. Datei, in die Meldungen von Programmen geschrieben wird
MIME	Multipurpose Internet Mail Extensions (deutsch: "Mehrzweck-Erweiterung für Internet-Post") sind Internet-Erweiterungen (Kodierungsverfahren), um binäre Daten in Internet-Emails einzubinden. Zusätzlich unterstützt MIME etwa so genannte Multipart-Emails, um in einer Email verschiedene Datentypen zu ermöglichen oder binäre Anhänge und Emails im HTML-Format.
MTA	Mail Transfer Agent: Programm, das den Versand von Emails über SMTP übernimmt, z. B. Sendmail, Postfix, Exim
Quarantäneverzeichnis	Verzeichnis, in das infizierte Dateien geschoben werden, um sie dem Zugriff der Benutzer zu entziehen (z. B. rejected)
root	Benutzer mit uneingeschränkten Rechten für die Systemverwaltung (entsprechend dem Administrator bei Windows)
Scan Engine	Modul der AntiVir-Software, das die Suche nach Viren und unerwünschten Programmen steuert
Skript	Textdatei mit Befehlen, die von UNIX ausgeführt werden. (Entspricht etwa einer Batchdatei bei DOS)

<b>Begriff</b>	<b>Erklärung</b>
SMTP	Simple Mail Transfer Protocol: Verfahren, auf dessen Basis Emails im Internet transportiert werden
syslog-Dämon	Dämon, der die Meldungen diverser Programme protokolliert. Die Meldungen werden in unterschiedliche Logdateien geschrieben. Die Konfiguration des syslog-Dämons wird in /etc/antivir.conf festgelegt.
Unerwünschte Programme	Oberbegriff für Programme, die keinen direkten Schaden auf Ihrem System verursachen oder ohne Absicht des Anwenders oder Administrators installiert wurden. Hierzu zählen Backdoor-Steuerprogramme (BDC), Dialer, Witzprogramme und auch Spiele.
VDF (Virus Definition File)	Virendefinitionsdatei: Datei mit den Signaturen der bekannten Viren und unerwünschten Programme. In vielen Fällen ist es für ein Update ausreichend, diese Datei zu aktualisieren.
Virendefinitionsdatei	siehe VDF

## 8.2 Weitere Infoquellen

Weitere Informationen zu verschiedenen Viren, Würmern, Makroviren und unerwünschten Programmen sind erhältlich unter <http://www.antivir.de>.

## 8.3 Goldene Regeln zur Virenvorsorge

- ▶ Erstellen Sie Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkserver und die einzelnen Workstations. Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- ▶ Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Disketten ohne ausführbare Programme enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- ▶ Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an.
- ▶ Begrenzen Sie den Programmaustausch: Das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- ▶ Prüfen Sie neue Programme vor und nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, lässt sich ein Virus bzw. unerwünschtes Programm in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu Ihrem Rechner, sollten Sie folgende Spielregeln zum Schutz vor Viren und unerwünschten Programmen beachten:

- ▶ Stellen Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerk-Medien) und von Downloads bereit. **Trennen Sie diesen Rechner aber vom Netzwerk!**
- ▶ Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist, und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus notwendigen Schritte.
- ▶ Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/Veränderungen aufgrund von Inkompatibilitäten vermindern helfen. Programme und Massenspeicher lassen sich ersetzen; Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- ▶ Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- ▶ Sorgen Sie für ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird. Es ist ein guter Schutz gegen Viren und unerwünschte Programme.



**Programm & Dokumentation**  
**Copyright © 2004**  
**H+BEDV Datentechnik GmbH**  
**Alle Rechte vorbehalten**

**Herausgeber:**  
**H+BEDV Datentechnik GmbH**  
**D-88069 Tettnang, Lindauer Strasse 21**

**Tel.: +49 (0) 7542 / 500 0**  
**Fax: +49 (0) 7542 / 52510**

**Internet: <http://www.antivir.de>**  
**<http://www.hbedv.com>**

**Ausgabe Februar 2005**